



Survey & Title Automation
Landonline

Certificate Policy

December

04

Table of Contents

- 1 INTRODUCTION..... 5**
 - 1.1.1 Overview..... 5*
 - 1.1.2 Document Structure..... 5*
 - 1.2 POLICY IDENTIFICATION..... 6
 - 1.3 COMMUNITY AND APPLICABILITY 6
 - 1.3.1 Registration Authority (LINZ) 6*
 - 1.3.2 Certificate Authority (beTRUSTed)..... 6*
 - 1.3.3 Subscriber (User) 6*
 - 1.3.4 Proof of Identity Certifier..... 6*
 - 1.3.5 Relying Parties 6*
 - 1.3.6 Trusted Contact..... 7*
 - 1.3.7 Applicability of Public Key Infrastructure Service..... 7*
 - 1.4 CONTACT DETAILS..... 7
- 2 GENERAL PROVISIONS 8**
 - 2.1 OBLIGATIONS 8
 - 2.1.1 Registration Authority Obligations 8*
 - 2.1.2 Proof of Identity Certifier Obligations 8*
 - 2.1.3 Certificate Authority Obligations 9*
 - 2.1.4 Subscriber Obligations..... 9*
 - 2.1.5 Relying Party Obligations 9*
 - 2.2 COMPLIANCE AUDIT..... 10
 - 2.2.1 Frequency of Compliance Audit..... 10*
 - 2.3 CONFIDENTIALITY 10
 - 2.4 INTELLECTUAL PROPERTY RIGHTS..... 11
- 3 IDENTIFICATION AND AUTHENTICATION 12**
 - 3.1 INITIAL REGISTRATION..... 12
 - 3.1.1 Types of Names..... 12*
 - 3.1.2 Authentication of Individual Identity..... 12*
 - 3.2 ROUTINE RE-KEY (RENEWAL) OF DIGITAL CERTIFICATES 13
 - 3.3 RE-KEY AFTER REVOCATION 13
 - 3.4 REVOCATION REQUEST 13
- 4 OPERATIONAL REQUIREMENTS..... 14**
 - 4.1 APPLICATION FOR SUBSCRIBER DIGITAL CERTIFICATE..... 14
 - 4.2 DIGITAL CERTIFICATE ISSUANCE 14
 - 4.3 DIGITAL CERTIFICATE ACCEPTANCE..... 14
 - 4.4 DIGITAL CERTIFICATE SUSPENSION / REVOCATION..... 15
 - 4.4.1 Circumstances for Revocation..... 15*
 - 4.4.2 Who Can Request Revocation..... 15*
 - 4.4.3 Procedure for Revocation Request..... 15*
 - 4.4.4 Certificate Revocation List Issuance Frequency 16*
 - 4.4.5 Certificate Revocation List Checking Requirements 16*
 - 4.4.6 Special Requirements Regarding Key Compromise 16*
 - 4.4.7 Certificate Update 16*
 - 4.5 SYSTEM SECURITY AUDIT PROCEDURES 16
 - 4.5.1 Types of Events Recorded..... 17*
 - 4.5.2 Frequency of Audit Log Processing 17*
 - 4.5.3 Retention Period for Audit Logs..... 17*
 - 4.5.4 Protection of Audit Log 17*
 - 4.5.5 Audit Logs Back-up Procedures..... 17*
 - 4.5.6 Audit Collection Systems 17*
 - 4.5.7 Notification to Event Causing Subject..... 17*
 - 4.5.8 Vulnerability Assessments 18*

- 4.5.9 *Certificate Management Records* 18
- 4.6 RECORDS ARCHIVE 18
 - 4.6.1 *Types of Events Recorded*..... 18
 - 4.6.2 *Retention Period for Archive*..... 18
 - 4.6.3 *Protection of Archive*..... 18
 - 4.6.4 *Archive Back-up Procedures*..... 19
 - 4.6.5 *Requirements for Date Stamping of Records* 19
 - 4.6.6 *Procedures to Obtain and Verify Archive Information* 19
- 4.7 ROUTINE RE-KEY..... 19
- 4.8 COMPROMISE AND DISASTER RECOVERY 19
 - 4.8.1 *Computing Resources, Software, and/or Data Are Corrupted*..... 20
 - 4.8.2 *Compromise of the Certification Authority Private Key (Key compromise plan)*..... 20
 - 4.8.3 *Certification Authority Cessation of Services*..... 20
- 5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS 21**
 - 5.1 PHYSICAL SECURITY CONTROLS 21
 - 5.1.1 *Site Location and Construction* 21
 - 5.1.2 *Physical Access* 21
 - 5.1.3 *Power and Air Conditioning* 21
 - 5.1.4 *Water Exposures*..... 21
 - 5.1.5 *Fire Prevention and Protection*..... 21
 - 5.1.6 *Media Storage* 21
 - 5.1.7 *Waste Disposal*..... 21
 - 5.1.8 *Off-site Storage*..... 22
 - 5.2 PROCEDURAL CONTROLS 22
 - 5.2.1 *Trusted Roles*..... 22
 - 5.2.2 *Number of Persons Required Per Task* 22
 - 5.2.3 *Identification and Authentication for the Registration Authority*..... 22
 - 5.2.4 *Landonline Procedural Change Controls* 23
 - 5.3 PERSONNEL SECURITY CONTROLS 23
 - 5.3.1 *Background, Qualifications, Experience, and Personnel Screening*..... 23
 - 5.3.2 *Background Check Procedures* 23
 - 5.3.3 *Training Requirements* 23
 - 5.3.4 *Retraining Frequency and Requirements*..... 24
 - 5.3.5 *Sanctions for Unauthorised Actions* 24
 - 5.3.6 *Documentation Supplied to Personnel* 24
- 6 TECHNICAL SECURITY CONTROLS..... 25**
 - 6.1 KEY PAIR GENERATION AND INSTALLATION 25
 - 6.1.1 *Key Pair Generation*..... 25
 - 6.1.2 *Private Key Delivery to Entity*..... 25
 - 6.1.3 *Public Key Delivery to Digital Certificate Issuer*..... 25
 - 6.1.4 *Certification Authority Public Key Delivery to Subscribers*..... 25
 - 6.1.5 *Key Sizes*..... 25
 - 6.1.6 *Hardware/Software Key Generation*..... 26
 - 6.1.7 *Key Usage Purposes (as per X.509v3 field)*..... 26
 - 6.2 PRIVATE KEY PROTECTION 26
 - 6.2.1 *Standards for Cryptographic Module*..... 26
 - 6.2.2 *Private Key (n out of m) Multi-person Control* 26
 - 6.2.3 *Private Key Escrow* 27
 - 6.2.4 *Private Key Back-up*..... 27
 - 6.2.5 *Private Key Archive*..... 27
 - 6.2.6 *Private Key Entry Into Cryptographic Module* 27
 - 6.2.7 *Method of Activating Private Key*..... 27
 - 6.2.8 *Method of Deactivating Private Key* 27
 - 6.2.9 *Method of Destroying Private Key* 27
 - 6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 28
 - 6.3.1 *Public Key Archive* 28
 - 6.3.2 *Usage Periods for the Public and Private Keys* 28

6.4	ACTIVATION DATA.....	28
6.4.1	Activation Data Generation and Installation.....	28
6.4.2	Activation Data Protection.....	28
6.5	COMPUTER SECURITY CONTROLS.....	28
6.5.1	Specific Computer Security Technical Requirements.....	28
6.5.2	Security Management Controls.....	29
6.5.3	Windows Operating Systems.....	29
6.5.4	Cryptographic Module Engineering Controls.....	30
6.5.5	Communications Infrastructure.....	30
6.5.6	Operating and Management Procedures.....	31
6.6	CERTIFICATE POLICY.....	31
6.6.1	Certificate Policy Object Identifier.....	31
7	DIGITAL CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES.....	32
7.1	DIGITAL CERTIFICATE PROFILE.....	32
7.1.1	Version Number.....	32
7.1.2	Digital Certificate Extensions.....	32
7.1.3	Algorithm Object Identifiers.....	32
7.1.4	Name Forms.....	33
7.1.5	Name Constraints.....	33
7.1.6	Certificate Policy Object Identifier.....	33
7.1.7	Usage of Policy Constraints Extension.....	33
7.1.8	Processing Semantics for the Critical Certificate Policy Extension.....	33
7.2	CERTIFICATE REVOCATION LIST PROFILE.....	33
7.2.1	Version Number.....	33
7.2.2	Certificate Revocation List and Certificate Revocation List Entry Extensions.....	33
8	SPECIFICATION ADMINISTRATION.....	34
8.1	SPECIFICATION CHANGE PROCEDURES.....	34
8.1.1	Items that Can Change Without Notification.....	34
8.1.2	Changes With Notification.....	34
8.1.3	Notification Mechanism.....	34
8.1.4	Comment Period.....	34
8.1.5	Mechanism to Handle Comments.....	34
8.1.6	Period for Final Change Notice.....	34
8.1.7	Items Whose Change Requires a New Policy.....	34
8.2	PUBLICATION AND NOTIFICATION PROCEDURES.....	35
9	GLOSSARY.....	36

1 INTRODUCTION

This document is the Land Information New Zealand Certificate Policy. It defines the rules by which keys and Digital Certificates are to be issued and managed within a Public Key Infrastructure. It is intended for use by managers, information technology owners, and others within the client community who need to determine the suitability of Digital Certificates issued under this Certificate Policy as a prerequisite to use the *Landonline* application. It also serves as the basis for the Registration Authority Public Key Infrastructure compliance inspection. Further, for individual users and other entities, it serves to describe the rights, roles, and responsibilities around the use of Digital Certificates.

Readers of this document can consult the Certification Practice Statement of the issuing Certification Authority, beTRUSTed, to obtain further details of the Certificate Authority's implementation of this Policy. This document is located at <http://www.betrusted.com/vault/terms>. beTRUSTed is a managed Public Key Infrastructure business within PricewaterhouseCoopers.

No stipulation is made for the following sections from the beTRUSTed Certification Practice Statement: 2.2, 2.3, 2.4, 2.5, 2.6, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 4.4.4, 4.7.1, 4.7.2, 4.9, 6.6, 6.7, 6.8, and 8.3.

This document is not intended as an educational document. The definition of roles and terms in the Glossary and the list below highlight the key Public Key Infrastructure terms used herein.

1.1.1 Overview

The class two (2) public and private keys and the Digital Certificates issued under this Certificate Policy are to be used for purposes of authentication, Digital Signatures, and non-repudiation.

This Certificate Policy identifies specific roles and responsibilities for the Registration Authority which manages the Digital Certificates. This Certificate Policy recognises the role of the Proof of Identity Certifiers who perform the "Proof of Identity" check. Subscribers and Relying Parties also have specific obligations that are outlined in this policy.

A prospective Subscriber must be authenticated in the manner set out in this policy by the Proof of Identity Certifier. When the Subscriber is set up they are accountable for the use of their Digital Certificates.

1.1.2 Document Structure

The format of this document follows the "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – March 1999" published by the Internet Engineering Task Force Request for Comments 2527.

Sections or subsections of Request for Comments 2527 not applicable to the *Landonline* Public Key Infrastructure framework are not included in this Certificate Policy document.

1.2 Policy Identification

This Certificate Policy is owned by Land Information New Zealand and has been assigned a Object Identifier of 1.3.6.1.4.1.6334.1.1.2.5.19.555001.

1.3 Community and Applicability

The *Landonline* Public Key Infrastructure comprises of five (5) distinct entities and the service that are responsible for the issuance, use and management of Digital Certificates.

1.3.1 Registration Authority (LINZ)

The Registration Authority is delegated responsibility from the Certificate Authority to manage all Subscribers under that approved Certificate Authority. The Registration Authority is responsible for the internal lifecycle management of Subscriber Digital Certificates. Tasks that are required to be performed by this entity will be performed by specific members of the Registration Authority. These Registration Authority personnel will perform Registration Authority operations in a secure facility using smartcard protected workstations.

1.3.2 Certificate Authority (beTRUSTed)

beTRUSTed is a managed, vendor neutral, Public Key Infrastructure service responsible for the generation and signing of Digital Certificates. As a Trusted Third Party, beTRUSTed provides Digital Certificates to use within the *Landonline* environment.

1.3.3 Subscriber (User)

Users of the *Landonline* external interface will be Subscribers. Subscribers may be issued keys and Digital Certificates for use with the *Landonline* application, provided that the responsibility and accountability is attributable to that individual through this Certificate Policy document, the beTRUSTed Certification Practice Statement document and any LINZ requirements.

1.3.4 Proof of Identity Certifier

Proof of Identity Certifiers are recognised by the Registration Authority to act in specific capacities for the Subscriber registration and revocation administration processes. LINZ allows all named groups under the Oaths and Declarations Act 1957 to act as Proof of Identity Certifiers, including Justices of the Peace, Solicitors and Commissioners for Oaths. Application for a digital certificate involves a proof of identity check. During the proof of identity check, the Proof of Identity Certifiers act to certify the Subscribers Government issued photo identification as a true copy.

1.3.5 Relying Parties

A Relying Party checks or relies on Digital Certificates issued under this Certificate Policy. Land Information New Zealand is the only Relying Party on the use of Digital Certificates as outlined in this policy.

1.3.6 Trusted Contact

A Trusted Contact is a member of a subscribing organisation or firm, who has the responsibility for registration and revocation assistance for that organisation, or firm's, personnel. An example of a Trusted Contact is a senior full-time Administrative Assistant.

1.3.7 Applicability of Public Key Infrastructure Service

The *Landonline* Public Key Infrastructure framework has been introduced to complement existing and proposed application's security controls. The framework is a combination of in-sourced (Land Information New Zealand) and out-sourced (beTRUSTed) functions, established to provide:

- Risk mitigation through authentication of Subscribers during logon; and
- Digital Signature lodgement capability on title instruments and survey transactions.

1.4 Contact Details

Queries relating to this document applicability and content should be forwarded to:

Address: Private Box 5501, Wellington.

Attn: (reference Title): Land Information New Zealand Registration Authority

Phone Number: 0800 ONLINE (665 463)

Email Address: solutions@linz.govt.nz

2 GENERAL PROVISIONS

The General Provision section contains Public Key Infrastructure entity obligations, compliance audit, and confidentiality policies.

2.1 Obligations

This section provides a general description of the roles and responsibilities of entities participating in the *Landonline* Public Key Infrastructure framework. Obligations are mandatory responsibilities for the particular entity.

2.1.1 Registration Authority Obligations

- i. Responsible for the acceptance of the Subscriber's valid Digital Certificate request.
- ii. Responsible for the Subscriber registration, re-key, and revocation procedures in accordance with this policy.
- iii. Responsible for the security controls of the Registration Authority system and Registration Authority workstation.
- iv. Responsible for maintaining appropriate records.
- v. Responsible for the investigation of the misuse of the Public Key Infrastructure.
- vi. Responsible for the monitoring and backing up of LINZ Registration Authority logs.
- vii. Responsible for the monitoring of the LINZ Registration Authority infrastructure.
- viii. Responsible for the continued update of the LINZ Certificate Policy document and other Public Key Infrastructure operations documents.
- ix. Responsible for Subscriber support.
- x. Responsible for notification of the Subscriber when a Digital Certificate bearing the Subscriber's Distinguished Name is issued or revoked.
- xi. Responsible for issuance of a Digital Certificate request only when the Registration Authority personnel certifies that the information stated in the Digital Certificate was verified in accordance with this Certificate Policy. Publication of the Digital Certificate in a repository, to which the Subscriber has access, constitutes notice of such verification.
- xii. Responsible for ensuring that the activation data expiry period does not exceed twenty-one (21) total days. There is no stipulation for the period between the receipt of a request for a Digital Certificate and the initialisation of the entity at the Certificate Authority.
- xiii. Responsible for ensuring that all private keys it holds or stores and the activation data are protected in accordance with sections **4 Operational Requirements** and **6 Technical Security Controls**.
- xiv. Responsible for checking the status of all Digital Certificates against the appropriate and current Certificate Revocation List in accordance with the requirements stated in section **4.4.5 Certificate Revocation List Checking Requirements**.
- xv. Responsible for ensuring that Subscribers are aware of their responsibilities under the Certificate Policy, the beTRUSTed Certification Practice Statement and any other LINZ policy documents that outlines the conditions of use.

2.1.2 Proof of Identity Certifier Obligations

- i. Responsible for complying with the Land Information New Zealand requirements that are detailed on the form provided during the "Proof of Identity" check in Subscriber registration.

2.1.3 Certificate Authority Obligations

- i. Responsible for operating in accordance with its beTRUSTed Certification Practice Statement and this Certificate Policy when issuing and managing Land Information New Zealand keys and Digital Certificates provided to Subscribers and Public Key Infrastructure personnel under this Certificate Policy.
- ii. Responsible for ensuring that notice of revocation of a Digital Certificate is posted to the Certificate Revocation List within the time limits stated in section **4.4.4 Certificate Revocation List Issuance Frequency**.
- iii. Responsible for ensuring the address of the Certificate Revocation List must be defined in the Digital Certificate.
- iv. Responsible for ensuring the signing private key, when used for Land Information New Zealand, is used only to sign Digital Certificates, Authority Revocation Lists and Certificate Revocation Lists for **Landonline**.
- v. Responsible for issuance of Land Information New Zealand Digital Certificates, only directly through the Registration Authority personnel, through a check with the Proof of Identity Certifier, to Subscribers, devices and applications.
- vi. Responsible for maintaining the Directory shadowing service to **Landonline**.
- vii. Responsible for maintaining Public Key Operations at the Certificate Authority side.
- viii. Responsible for the Global Help Desk for use by the Registration Authority.

2.1.4 Subscriber Obligations

- i. Responsible for providing Government photo identification for “Proof of Identity” during registration.
- ii. Responsible for providing a photocopy of Government photo identification on the form provided during registration.
- iii. Responsible for key generation through the Land Information New Zealand approved cryptographic module and on-line acceptance of their Certificate Authority-signed Digital Certificate as per the Land Information New Zealand registration process.
- iv. Responsible for secure use and management of Digital Certificate.
 - v. Responsible for communicating any concerns associated with the integrity, validity, or change of their Digital Certificate immediately to the Land Information New Zealand Registration Authority personnel.
 - vi. Responsible for using Digital Certificates for **Landonline** purposes only.
 - vii. Responsible for their own Digital Certificates.
- viii. Responsible for their tasks in this Certificate Policy and any other Land Information New Zealand policy documents.
- ix. Responsible for submission of complete and accurate information to Registration Authority personnel and Proof of Identity Certifiers in connection with Digital Certificates.
- x. Responsible for protecting their keys and Digital Certificates in accordance with section **6 Technical Security Controls** and to take all reasonable measures to prevent their loss, disclosure, modification or unauthorised use.
- xi. Responsible for notification, on suspicion of any Digital Certificate compromise, the issuing Registration Authority personnel, in a manner specified by the Land Information New Zealand Registration Authority and by the **Landonline** support material.

2.1.5 Relying Party Obligations

- i. Responsible for, prior to using a Digital Certificate, checking the status of the Digital Certificate against the appropriate and current Certificate Revocation List in accordance with the requirements stated in section **4.4.5 Certificate Revocation List Checking**

Requirements. As part of this verification process, the Digital Signature of the Certificate Revocation List must also be validated.

2.2 Compliance Audit

- i) The compliance review of **Landonline** Public Key Infrastructure environment will be performed by beTRUSTed or as coordinated by the Registration Authority personnel.
- ii) The internal review will comprise of the assessment of the **Landonline** Public Key Infrastructure associated hardware and software and operational and management procedures. These include:
 - Technical security reviews of the platforms supporting the Registration Authority and **Landonline** Public Key Infrastructure components.
 - Assessment of the Registration Authority and **Landonline** Public Key Infrastructure system configuration.
 - Assessment of monitoring controls to ensure they are appropriate for current requirements.
 - Assessment of operational and management procedures over the registration and continued management of Digital Certificates.
 - Assessment of Registration Authorities and **Landonline** Administrator compliance over this Certificate Policy and other related policy documentation.
- iii) Responsibility for the compliance audit of **Landonline** Public Key Infrastructure will reside with Land Information New Zealand.
- iv) Required audit activities to assess the integrity and control of **Landonline** Public Key Infrastructure will be established by Land Information New Zealand and beTRUSTed and will be linked to the performance of associated audit reviews.

2.2.1 Frequency of Compliance Audit

Land Information New Zealand shall undergo audits from time to time to review the compliance of Land Information New Zealand with its obligations under this Certificate Policy. Specific activities and timings are:

- i) Compliance review of Registration Authority **Landonline** infrastructure shall be conducted on an annual basis.
- ii) Compliance audit of **Landonline** Public Key Infrastructure shall be conducted whenever there is a significant change to this Certificate Policy, the beTRUSTed Certification Practice Statement, or the operations at beTRUSTed on behalf of Land Information New Zealand.

2.3 Confidentiality

Confidential Subscriber, Public Key Infrastructure and Registration Authority information shall only be disclosed and otherwise dealt with in accordance to existing Land Information New Zealand Customer Contracts and New Zealand law. Any information about an individual from which their identity is apparent or can reasonably be ascertained is considered confidential.

This includes, but is not limited to: documents, databases, photographs, or other pictorial representation of a person.

2.4 Intellectual Property Rights

Land Information New Zealand owns the Intellectual Property Rights to this Certificate Policy and any associated Registration Authority and Public Key Infrastructure policy documentation.

3 IDENTIFICATION AND AUTHENTICATION

The identification and authentication section sets out the identification requirements for the authentication process prior to Subscriber receiving the Digital Certificate in the registration process.

3.1 Initial Registration

3.1.1 Types of Names

The Subscriber's User ID listed in the Digital Certificate shall be unambiguous and unique for all Land Information New Zealand Digital Certificates issued by the Certificate Authority. It shall comprise a concatenated string, made up of:

- Initial of their first name + Surname + if necessary, additional numbers will be appended to this string ensure the name's uniqueness within the domain of Digital Certificates issued for **Landonline**. For example, a second subscriber with the name Sharon Brown may have a User ID of SBrown002.

Each Subscriber must have a clearly distinguishable and unique Distinguished Name in the Digital Certificate subject name field of the associated Digital Certificate. The Distinguished Name must be in the following format and must not be blank:

- - Distinguished Name of each Subscriber = CN:<User ID>,OU:LINZ,O:beTRUSTed,C:NZ
 - Distinguished Name of issuing Certificate Authority = CN:beTRUSTed Class 2 CAYY,CN:Entrust,O:beTRUSTed,C:WW

Subscriber Common Names will be re-issued in the case of procedures including "re-registration" and a "routine re-key", so that the initial Common Name of a particular **Landonline** Subscriber will not change during their entire lifetime of usage of **Landonline**. This is required for a security check that is performed during authentication.

3.1.2 Authentication of Individual Identity

Identification and authentication of the individual must be through the following means:

- The Proof of Identity Certifier will verify the identity of the individual using a Government photo identification containing a photo and will sign the official Land Information New Zealand form.
- The Proof of Identity Certifier will record the unique identification information associated with Government photo identification, such as passport number or driver's license number, on the official LINZ form.
- The Registration Authority personnel must keep an archive of the Subscriber Request forms and all relevant documentation that are provided (i.e. by fax, mail).

If the identity of an individual has previously been established through a full user Digital Certificate registration and the identification used is still current, the “routine re-key” to get new keys and Digital Certificates does not require the rigorous steps as in the “single user Digital Certificate registration”, because the Subscriber is already an established Subscriber.

3.2 Routine Re-key (Renewal) of Digital Certificates

The Registration Authority personnel must authenticate all re-key operations as per the Registration Authority “Routine re-key” process. Subscriber “Proof of Identity” forms that include details of the unexpired Government photo identification used with the original submitted form are required. The activation data will then be split up to two (2) known business email addresses as part of this procedure.

3.3 Re-key After Revocation

Where the information contained in a Digital Certificate has changed, or there is a known or suspected compromise of the private key (or the matching Digital Certificates stored in the Internet browser), the Registration Authority personnel must authenticate the complete “user Digital Certificate registration” in the same manner as for initial registration.

In the case of the “Proof of Identity” form previously completed by the Subscriber and archived by the Registration Authority personnel still being within the validity period for the ID used, a new “Proof of Identity” form is not required. A new “Proof of Identity” form may still be required in certain cases, at the discretion of the Registration Authority personnel.

3.4 Revocation Request

The Registration Authority personnel must authenticate a request for revocation of a Digital Certificate. Requests for revocation of a Digital Certificate must be logged.

The Revocation request will contain information regarding the Digital Certificate to be revoked including: the time and date, the reason, the Common Name from the Digital Certificate, and the requestor.

4 OPERATIONAL REQUIREMENTS

This section outlines the steps and policies for the operation of the Land Information New Zealand Registration Authority.

4.1 Application For Subscriber Digital Certificate

Any individual applying for a *Landonline* Digital Certificate must complete the following general procedures for each Digital Certificate application. The following steps are used in all cases:

- i) Trusted Contact initiates the Subscriber application process with Land Information New Zealand.
- ii) Subscriber provides a legible photocopy of their Government photo identification, the original Government photo identification and the Subscriber application form, available from the Land Information New Zealand website, to a Proof of Identity Certifier who will verify them.
- iii) The Subscriber provides the verified application form to the Registration Authority personnel.

4.2 Digital Certificate Issuance

Upon successful completion of the Subscriber's identification and authentication process in accordance with this Certificate Policy and the approval of Digital Certificate request by the Registration Authority personnel, the Registration Authority personnel will issue the requested activation data for the Digital Certificate.

- i) Half of the activation data will be e-mailed to the Subscriber and half to the Trusted Contact. In the case of only one (1) Subscriber at the Firm, one (1) half of the activation data is emailed to the Subscriber and the Subscriber must then telephone the Registration Authority personnel to receive the other half verbally.
- ii) The Digital Certificate URL will prompt the Subscriber to download the Digital Certificate to the local Internet browser. The private and public keys are immediately created from the local Internet browser in the Subscriber's workstation.
- iii) Download of Digital Certificate will be performed via a secure server side Secure Sockets Layer protected link between the Subscriber and the beTRUSTed site.

4.3 Digital Certificate Acceptance

On receipt of the Digital Certificate, the Subscriber shall be responsible for checking that the Digital Certificate has not been damaged or corrupted during transit as outlined in the support documentation.

- i) The Subscriber will check the Digital Certificate for correctness and then use the Digital Certificate in a secure manner for *Landonline* use only.

- ii) In the event that the Digital Certificate is damaged or corrupted, the Subscriber shall contact the Registration Authority personnel and request another Digital Certificate.
- iii) In the event of any actual or suspected loss, disclosure or other compromise of the Subscriber's private key (and associated Digital Certificate in the Internet browser), the Subscriber shall request that the Digital Certificate be revoked and new Digital Certificate can be requested.

4.4 Digital Certificate Suspension / Revocation

4.4.1 Circumstances for Revocation

A Digital Certificate must be revoked if:

- A Subscriber has lost a Digital Certificate through a file loss, corruption, or a re-build of their workstation.
- A Subscriber suspects that their Digital Certificate has been compromised (e.g. gave a copy away, left a machine unattended with password available, or suspects someone has a copy).

The Registration Authority personnel will revoke a Digital Certificate when the entity fails to comply with obligations set out in this Certificate Policy, the beTRUSTed Certification Practice Statement, any other agreement, other Land Information New Zealand Policy document, or any applicable law.

4.4.2 Who Can Request Revocation

The revocation of a Digital Certificate may only be requested by:

- The Subscriber in whose name the Digital Certificate has been issued;
- The Trusted Contact Person of the Organisation who made the application for the Digital Certificate on behalf of a the Subscriber;
- A Senior Manager of the Firm;
- Registration Authority personnel; or
- beTRUSTed.

4.4.3 Procedure for Revocation Request

An authenticated revocation request and all resulting actions taken by the Registration Authority personnel must be recorded and retained.

- Where a Digital Certificate is revoked, full justification for the revocation must also be documented.
- Where a Subscriber, device, or Registration Authority personnel Digital Certificate is revoked, the revocation must be published in the appropriate Certificate Revocation List.
- All Digital Certificate revocation requests will be communicated to the Registration Authority.
- Digital Certificate revocations can be requested over the telephone and suspended immediately.

- It must be followed by supporting documentation from authorised party after being requested. A suspension is the immediate first step which places the Digital Certificate on the Certificate Revocation List, but which can be reversed by the Registration Authority.
- Revocation requests must be processed immediately, after the request being validated.
- The revocation of the Digital Certificate must be communicated to the Subscriber as soon as it has taken place. The Subscriber shall be communicated with e-mail and the Registration Authority personnel will retain a copy of the notification.

4.4.4 Certificate Revocation List Issuance Frequency

The Certificate Authority must ensure that it issues an up to date Certificate Revocation List at least every twenty-four (24) hours. The Certificate Authority must also ensure that new Certificate Revocation Lists are synchronised with any Land Information New Zealand directory synchronisation and shadowing to ensure the accessibility of the most recent Certificate Revocation List to relying parties. When a Digital Certificate is revoked due to key compromise, the updated Certificate Revocation List must be issued immediately.

4.4.5 Certificate Revocation List Checking Requirements

Land Information New Zealand, as the only Relying Party, must check the status of all Digital Certificates in the Digital Certificate validation chain against the current Certificate Revocation Lists prior to their use. The authenticity and integrity of Certificate Revocation Lists is also checked.

4.4.6 Special Requirements Regarding Key Compromise

In the event of a compromise, or suspected compromise, of the Certificate Authority signing key, the Certificate Authority must immediately notify the Registration Authority personnel.

In the event of the compromise, or suspected compromise, of any other entity's signing key (or their associated Digital Certificate in the Internet browser), the entity must immediately notify the Registration Authority personnel.

The Certificate Authority must ensure that its beTRUSTed Certification Practice Statement or a publicly available document and appropriate agreements contains provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.4.7 Certificate Update

An update of the Subscriber's Digital Certificate shall be considered a "routine re-key" process as detailed in section 3.2 Routine Re-key (Renewal).

4.5 System Security Audit Procedures

Land Information New Zealand will implement and maintain Trustworthy Systems to preserve an audit trail for all Material Events for the Registration Authority such as logon/logoff, certificate request, certificate revocation, etc. All electronic and hardcopy records will be

maintained through a thorough strict internal processes, physical and logical security controls, and weekly off-site back-ups. Land Information New Zealand will audit these procedures on an annual basis.

The audit processes can be audited by the Certificate Authority, provided that adequate notice is provided to Land Information New Zealand.

4.5.1 Types of Events Recorded

The Registration Authority personnel must record in audit log files all material events relating to the security of the Registration Authority system. All logs, whether electronic or manual, will contain the date and time of the event and the identity of the entity which caused the event.

To facilitate decision making, all agreements and correspondence relating to Registration Authority services must be collected and consolidated, either electronically or manually, at the Registration Authority site in Wellington.

4.5.2 Frequency of Audit Log Processing

The Registration Authority personnel must review audit logs at least on a weekly basis. Such reviews involve verifying that the log has not been tampered with, briefly inspecting all log entries and a more thorough investigation of any alerts or irregularities in the logs.

Supporting logs from the Certificate Authority and Registration Authority must be compared when any action is deemed suspicious.

4.5.3 Retention Period for Audit Logs

The Registration Authority personnel will retain audit logs regarding material events on-site for at least one (1) year from the date the audit logs were created and then they shall be archived.

4.5.4 Protection of Audit Log

The electronic audit log system must include mechanisms to protect the log files from unauthorised viewing, modification and deletion. Manual Registration Authority and Certificate Authority audit information must be protected from unauthorised viewing, modification and destruction.

4.5.5 Audit Logs Back-up Procedures

Audit logs and audit summaries must be backed up, or copied if in paper-based form.

4.5.6 Audit Collection Systems

The Registration Authority personnel will use the internal Help Desk system and Registration Authority workstation logs for audit collection purposes.

4.5.7 Notification to Event Causing Subject

If an event is logged by the audit collection system, no notice must be given to the **Landonline** individual, Organisation, device or application that caused the event.

4.5.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The Registration Authority personnel must ensure that a vulnerability assessment is performed, reviewed and revised following a security examination of these monitored events.

4.5.9 Certificate Management Records

The Registration Authority Digital Certificate management activities must be recorded and archived according to Land Information New Zealand's record keeping policy.

At a minimum, information related to the following activities shall be kept:

- i) Subscriber's registration;
- ii) Verification of Subscriber identity; and
- iii) Digital Certificate approval / revocation.

4.6 Records Archive

4.6.1 Types of Events Recorded

The Registration Authority personnel shall maintain and make available to the Certificate Authority, upon request, records relating to the performance of its obligations under the Customer Agreement and the Certification Practice Statement including:

- i) documentation of the Subscribers compliance with the Certificate Policy and the beTRUSTed Certification Practice Statement; and
- ii) documentation of actions and information that relate to each Digital Certificate application and to the creation, issuance, use, revocation, expiration, and renewal or re-key of each Digital Certificate relating to individuals it has authenticated. These records shall include all relevant evidence in the Registration Authority's possession regarding:
 - the identity of the Subscriber named in each Digital Certificate;
 - the identity of persons requesting Digital Certificate revocation;
 - other facts represented in the Digital Certificate; and
 - time stamps.

4.6.2 Retention Period for Archive

The Registration Authority personnel shall retain the archive records for at least seven (7) years (or six (6) years after the one (1) year specified in section 4.5.3 Retention Period for Audit Logs for any logs not backed up by the Certificate Authority) as indicated in the New Zealand National Archives Act 1957. Such records may be retained as retrievable computer-based messages or paper-based documents.

4.6.3 Protection of Archive

The Registration Authority personnel shall protect the archives of the records in a Trustworthy System that reasonably ensures the archive's integrity. Archive integrity shall be preserved

using Digital Signatures and other trustworthy methods. The Registration Authority personnel will periodically verify the integrity of the archives.

4.6.4 Archive Back-up Procedures

The audit logs shall be backed up in a manner consistent with this Certificate Policy.

4.6.5 Requirements for Date Stamping of Records

The Registration Authority personnel are obligated to date all records with a reasonably accurate time stamp at the time of creation of those records.

4.6.6 Procedures to Obtain and Verify Archive Information

In the event that the Certificate Authority determines that access to the Registration Authority's record archives is required, the Certificate Authority shall provide at least seven (7) days notice prior to such access wherever reasonable or practicable to do so. The Registration Authority shall provide all records requested in addition to any keys necessary to verify archive information. Should the archive records be in question, Land Information New Zealand will be obligated to provide documentation demonstrating trustworthiness of the archives.

4.7 Routine Re-Key

The Registration Authority will attempt to contact the subscriber by all reasonable methods, including e-mail, 28 days prior to the expiration of the subscribers certificate to initiate the Digital Certificate renewal process. The subscriber may initiate the process but may only apply to renew their Digital Certificate within three (3) months prior to the expiration of the Digital Certificate, provided the previous Digital Certificate has not been revoked.

Subscribers without a valid Digital Certificate or without valid "Proof of Identity" forms must be re-authenticated by the Registration Authority personnel and a Proof of Identity Certifier in the same manner as the initial registration.

Where a Subscriber's Digital Certificate has been revoked as a result of non-compliance, the Registration Authority personnel must verify that any reasons for non-compliance have been addressed to its satisfaction prior to Digital Certificate re-issuance. If it has been revoked, the Digital Certificate will require a complete re-registration, but the existing "Proof of Identity" form can be re-used, if still current.

Automated key and Digital Certificate changeover is permitted, but only the Land Information New Zealand Registration Authority personnel can do this. An automated key changeover means the Registration Authority personnel keys and Digital Certificates are updated automatically and securely on behalf of the Registration Authority personnel onto their smart card.

4.8 Compromise and Disaster Recovery

The Certificate Authority shall implement, document and periodically test such contingency planning and disaster recovery capabilities and procedures as it considers appropriate in light of its obligations under the beTRUSTed Certification Practice Statement.

4.8.1 Computing Resources, Software, and/or Data Are Corrupted

In the event that the Registration Authority's computing resources, software and/or data are corrupted, the Registration Authority personnel shall initiate a full recovery of all resources. A full recovery is defined as the Customer restoring computing resources to a state no more than twenty-four (24) hours older than the corrupted resource. Since the standard Registration Authority audit logs are backed up at the Certificate Authority, the only files that must be backed up are daily Registration Authority records kept on the Registration Authority workstations.

In the event that the Certificate Authority's computing resources, software and/or data is corrupted, the Certificate Authority shall use reasonable efforts to provide Digital Certificate services from a back-up location within twenty-four (24) hours of the corruption that occurred.

4.8.2 Compromise of the Certification Authority Private Key (Key compromise plan)

The Certificate Authority shall maintain a plan for dealing with the eventuality that the Certificate Authority private key is compromised. That plan shall accord with industry best practice and shall be updated regularly. Such plan shall include procedures for:

- i) Request that any signer Digital Certificates related to this key be revoked;
- ii) Revoking all Digital Certificates signed with this key; and
- iii) Promptly notifying all Subscribers to its services and all known relying parties.

4.8.3 Certification Authority Cessation of Services

In the event that the Certificate Authority ceases operation, it must notify its Subscribers prior to the termination of operations and arrange for the continued archiving of the Certificate Authority's keys and information. It must also notify all Certificate Authorities with which it is cross-certified.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The Registration Authority site must:

- Be located in it's own physically restricted operations zone with swipe card access.
- Be manually or electronically monitored for unauthorised intrusion at all times.
- Ensure a site access log is maintained and inspected periodically. This log will record all visits to the room.

The Registration Authority workstation must be located in an operations zone while attended, with all media protected when unattended. The Registration Authority personnel will ensure that the site provides appropriate security protection of the cryptographic module, all system software and the Registration Authority personnel Digital Certificates and keys.

5.1.2 Physical Access

Registration Authority personnel must not leave their workstations unattended when the cryptographic system is in an unlocked state (i.e. when the PIN or password has been entered).

Physical access to the Registration Authority room will be restricted and controlled through swipe card access, logs and monitoring.

5.1.3 Power and Air Conditioning

The Registration Authority personnel must ensure that the power and air conditioning facilities are sufficient to support the operation of the Registration Authority system.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

The Registration Authority personnel must ensure that storage media used by the Registration Authority system is protected from environmental threats such as temperature, humidity and magnetism.

5.1.7 Waste Disposal

All media used for the storage of information such as keys, Digital Certificates, activation data, or other files are to be sanitised or destroyed before released for disposal.

Printed material containing designated information must be disposed of in accordance with Land Information New Zealand policies and procedures.

5.1.8 Off-site Storage

The Registration Authority personnel must ensure that facilities used for off-site back-up or storage have the same level of security as the primary Registration Authority site.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors and consultants of **Landonline** that have access to or control over Material Events are considered as being in a Trusted Role in terms of the management of Digital Certificates at **Landonline**. Such personnel include, but are not limited to:

- Information Technology Support personnel;
- system (and site) security officers;
- system auditors; and
- Registration Authority personnel.

5.2.1.1 Trusted Roles for Registration Authority personnel

Registration Authority personnel must understand their responsibility for the identification and authentication of prospective Subscribers and that they perform the following functions:

- Acceptance of registration, Digital Certificate changes, re-key and revocation requests;
- Transmission of applicant information to the Certificate Authority during Digital Certificate issuance and revocation; and
- The Certificate Authority may permit all duties for Registration Authority functions to be performed by one (1) individual.

5.2.2 Number of Persons Required Per Task

All daily administrative duties associated with Registration Authority roles may be performed by an individual operating alone. Creating or revoking Registration Authority personnel requires two (2) authorisations and the presence of the Registration Authority Manager.

5.2.3 Identification and Authentication for the Registration Authority

All Registration Authority personnel must have their identity and authorisation verified before they are:

- Included in the access list for the Registration Authority site;
- Included in the access list for physical access to the Registration Authority system;
- Given a Digital Certificate for the performance of their Registration Authority role; and

- Given an account on the Public Key Infrastructure system.

Each of these Digital Certificates and accounts must:

- Be directly attributable to an individual;
- Not be shared; and
- Be restricted to actions authorised for that role through the use of Registration Authority software, operating system and procedural controls.

Registration Authority personnel are authenticated, once set up, to their smartcards so that they can use their RA workstations.

5.2.4 Landonline Procedural Change Controls

Change management controls must be in place to ensure all changes to the **Landonline** Public Key Infrastructure are formally approved before changes are implemented.

Security updates to the Registration Authority workstation software must be implemented when the software supplier identifies vulnerabilities and fixes are made available.

5.3 Personnel Security Controls

The Registration Authority personnel must ensure that all personnel performing duties with respect to the operation of a Registration Authority must:

- Be made aware and responsible for their daily Registration Authority functions and responsibilities.
- Have received comprehensive training with respect to the duties they are to perform.
- Be bound by contract not to disclose designated Registration Authority or Subscriber information.
- Not be assigned duties that may cause a conflict of interest with their Registration Authority duties.

5.3.1 Background, Qualifications, Experience, and Personnel Screening

The Registration Authority Manager must ensure that all personnel performing duties with respect to the operation of a Registration Authority have the appropriate qualifications and experience for the role.

5.3.2 Background Check Procedures

Background checks must be performed as per standard Land Information New Zealand security screening procedures.

5.3.3 Training Requirements

The Registration Authority Manager must ensure that all personnel performing duties with respect to the operation of the Registration Authority receive comprehensive training in:

- The Registration Authority security principles and mechanisms.
- All Public Key Infrastructure software versions in use on the Registration Authority system.
- All Public Key Infrastructure duties they are expected to perform.
- Registration Authority disaster recovery and business continuity procedures.
- All Registration Authority workstation dependent software, such as the Remedy system, that is also required in the Registration Authority role.
- Physical security training.

5.3.4 Retraining Frequency and Requirements

The purpose of retraining for the Registration Authority personnel is to keep the knowledge of these personnel current to accommodate changes in the Registration Authority system. The Registration Authority Manager must review requirements at least once a year and conduct refresher training as required.

5.3.5 Sanctions for Unauthorised Actions

In the event of actual or suspected unauthorised action by a person performing duties with respect to the operation of a Registration Authority personnel or Proof of Identity Certifier, the individual may have their access to the Certificate Authority revoked.

5.3.6 Documentation Supplied to Personnel

The Registration Authority personnel shall be provided with comprehensive documentation detailing the procedures for registration, re-keying and revocation of Subscribers.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each prospective Subscriber or other entity must initiate the generation of their own key pair, using a key type and length of at least RSA 1024. The associated Digital Certificate will be returned later by the Certificate Authority, as part of the registration process.

6.1.2 Private Key Delivery to Entity

The Subscriber shall never be required to deliver the private key used for Digital Signatures to the Certificate Authority.

The Registration Authority personnel shall never be required to deliver their private signing key to the Certificate Authority.

6.1.3 Public Key Delivery to Digital Certificate Issuer

The Subscriber's public key will be automatically delivered to the Certificate Authority at the time the Subscriber enters the activation data into their Digital Certificate Installation application. At this time, the public key is signed and returned to the Subscriber as a Digital Certificate. A copy is also kept by the Certificate Authority and is posted to the Certificate Authority Master Directory. The delivery channel will be protected by Secure Sockets Layer process.

The Registration Authority personnel public keys and encryption private keys¹ are also stored at the Certificate Authority for back-up purposes. This occurs upon entry of the activation data and with the two (2) Registration Authorisations that are required. The delivery is protected by a proprietary symmetric key encrypted channel.

6.1.4 Certification Authority Public Key Delivery to Subscribers

The Certificate Authority public verification key must be delivered to the prospective Digital Certificate holders in an on-line transaction in a protected Secure Sockets Layer session.

The Certificate Authority public verification key must be delivered to the Registration Authority personnel as part of their normal symmetric encryption session.

6.1.5 Key Sizes

The Certificate Authority must ensure that the key pairs for all entities are at least 1024 bit RSA.

¹ All Registration Authority keypairs are dual keys. One key is used for signing, the other is used for encryption. Encryption keys are backed up in this instance to provide escrow in the event of key loss.

6.1.6 Hardware/Software Key Generation

Subscribers will use software key generation technology through their Digital Certificate Installation application and use their hard disks for storage of their keys and Digital Certificates.

Land Information New Zealand Registration Authority personnel will use hardware cryptographic modules and smart cards.

6.1.7 Key Usage Purposes (as per X.509v3 field)

Key Usage describes the purpose of key pairs and Digital Certificates. The *Landonline* subscribers' keys pairs and Digital Certificates are to be used only for Digital Signatures and non repudiation. This is recorded in the Digital Certificate KeyUsage field in accordance with Public-Key Infrastructure X.509 Part 1 Digital Certificate and Certificate Revocation List Profile. Subscribers will also use their keys and Digital Certificates for authentication to *Landonline*, but this is not recorded as a KeyUsage value in the Digital Certificate.

Registration Authority personnel keys and Digital Certificates will be used in a range of authentication and signing functions to fulfil Registration Authority responsibilities, including daily Subscriber administration and accessing audit logs.

6.2 Private Key Protection

Each Subscriber applicant shall securely generate their own key pair, using their Digital Certificate Installation application browser's cryptographic module, and shall take all necessary precautions to prevent its loss, disclosure, modification, unauthorised use or other compromise.

The Registration Authority private keys are PIN or password protected on individual smart cards.

6.2.1 Standards for Cryptographic Module

Subscriber's Class 2 Digital Certificates must be stored on disk media (hard disk drive, or temporarily on floppy disk when relocating to another computer) and best efforts must be taken to prevent access to the Digital Certificate.

Each Registration Authority Class 2 Digital Certificate must be stored on an individual smart card.

6.2.2 Private Key (n out of m) Multi-person Control

Multiple person control for Subscribers is not required.

Multiple person control is required for Registration Authority key generation or revocation operations. The Registration Authority Manager and two (2) Registration Authority personnel must be present. The second Registration Authority personnel must be present when the Registration Authority is being added, since this is a "sensitive action" and requires two (2) Registration Authority authorisations. The Registration Authority Manager supervises this sensitive action.

6.2.3 Private Key Escrow

Private signing keys must not be escrowed by any entity. Subscribers must not use a third party escrow service to hold a copy of their Digital Certificates.

6.2.4 Private Key Back-up

Subscriber private keys contained within the Internet browser or the PKCS#12 file (the file which also contains the same private key and is used in signing functions in *Landonline*) may be routinely copied for disaster recovery back-up purposes .

The Registration Authority personnel are not to back up their private signing keys. The Certificate Authority will maintain this key back-up, not including the private signing key, on behalf of all Registration Authority personnel.

6.2.5 Private Key Archive

All entities may not keep copies of their private keys for archive purposes.

6.2.6 Private Key Entry Into Cryptographic Module

No stipulation for Subscribers.

Registration Authority personnel will create the private key directly on the cryptographic module on the smart card.

6.2.7 Method of Activating Private Key

No stipulation for Subscribers.

Registration Authority must be authenticated to the cryptographic module by an Operating System or Network Operating System level password before usage of the private key for *Landonline* functions.

6.2.8 Method of Deactivating Private Key

Subscriber's private keys will expire automatically one (1) year after issuance.

Registration Authority keys will automatically and securely rollover onto new keys when the Registration Authority personnel is authenticated to the Public Key Infrastructure, prior to expiry or on their next logon to the Registration Authority workstation.

6.2.9 Method of Destroying Private Key

Subscribers will delete their old Digital Certificates.

Registration Authority personnel will "zeroize" tokens if and when they are to be re-used. Alternatively, previously used Registration Authority smart cards will be securely destroyed under the supervision of the Registration Authority Manager.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archive

The issuing beTRUSTed Certificate Authority must archive all public verification keys for the lifetime of *Landonline*.

6.3.2 Usage Periods for the Public and Private Keys

Subscriber keys and Digital Certificates of 1024 bits must have validity periods of no more than one (1) year.

Registration Authority keys and Digital Certificates of a minimum of 1024 bits are to have a validity of no more than two (2) years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Any activation data must be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where passwords are used, an entity must have the capability to change their password at any time.

6.4.2 Activation Data Protection

Data used for entity initialisation must be protected from unauthorised use by a combination of cryptographic and physical access control mechanisms.

6.5 Computer Security Controls

This section of the document covers the components of the *Landonline* Public Key Infrastructure configuration that require review by Registration Authority personnel on an annual basis to ensure the security and integrity of the *Landonline* Public Key Infrastructure configuration.

The key components discussed within this section are the operating system, communications, application software, and operating and management procedures. These are considered the major areas in which control weaknesses would have the most detrimental effect.

6.5.1 Specific Computer Security Technical Requirements

Each Registration Authority system must include the following functionality, either provided by the operating system, or through a combination of operating system, Registration Authority application and physical safeguards:

- Access control to Registration Authority services;
- Smart card protected Registration Authority workstations;
- Separation of duties between Registration Authority and System Administrators;
- Identification and authentication of Registration Authority role;

- Archive of Registration Authority and entity history and audit data;
- Audit of security related events;
- Self-test of security related Registration Authority services;
- Recovery mechanisms for keys and the Registration Authority system.

6.5.2 Security Management Controls

The Registration Authority software, when first loaded, must provide a method for the Registration Authority to verify that the software on the system:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the version intended for use.

The Registration Authority system must provide a mechanism to periodically verify the integrity of the software.

6.5.3 Windows Operating Systems

While the Registration Authority and *Landonline* server-side Public Key Infrastructure configuration does not directly modify the operating system, its assessment is still considered fundamental to the compliance review, as all other components rely on its integrity and availability.

The following Registration Authority areas shall be reviewed:

6.5.3.1 Operating System Version

A review of the operating system, service packs and patches versions must be conducted in order to determine if any upgrades need to be applied to reduce the vulnerability of the system to known exploits.

6.5.3.2 User and Group Management

A review of users and group access must be performed to ensure access rights which have been granted are in line with users and group job responsibilities.

6.5.3.3 Password Management

A review of the password policies against best practice must be conducted to ensure they have been appropriately configured.

6.5.3.4 File System Access and Management

A review of the file protection of critical system resources and applications must be performed to ensure access is adequately restricted.

The removal of software that is no longer required & disablement of non-required services must also be performed.

6.5.3.5 Sensitive System Privileges and Utilities

A review of the privileges surrounding system utilities must be conducted to ensure that only authorised users have the ability to utilise administrative utilities. Only authorised personnel must be granted access to these utilities.

6.5.3.6 Maintenance and Operations

A review of the change control process for the operating system must be conducted. Appropriate methodologies must be in place for change control and adequate separation of development and production environments must be established.

6.5.3.7 Back-up and Recovery

A review of the back-up and recovery procedures must be undertaken to ensure the adequacy of this process. Procedural information must exist as to how to perform this activity. Additionally, logs of the performance and the success/failure of back-ups must be maintained and reviewed.

6.5.3.8 Physical Access

Access controls to the computer room housing the servers must be reviewed (eg. access card to gain access, limited to authorised personnel only, review those with access). Additionally, environment systems (eg. fire detection, temperature control, Uninterruptible Power Supply, generator) must be tested on a regular basis to ensure availability. The evidence of this testing must be reviewed.

6.5.3.9 Audit Logging and Monitoring

A weekly review of the system security audit logs must be performed to identify unauthorised access attempts. A review must be conducted to ensure that this activity is conducted and exceptions are adequately investigated and appropriate action taken.

6.5.4 Cryptographic Module Engineering Controls

All Registration Authority Digital Signature key generation, Registration Authority Administrator Digital Signature key storage, Digital Certificate signing operations, and other operations must be performed in a hardware cryptographic module rated to at least United States Federal Information Processing Standards 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

6.5.5 Communications Infrastructure

A review of the communications infrastructure is required to ensure that the Registration Authority workstations and applications are adequately protected from unauthorised access attempts and that appropriate ports have been opened to establish external connections for the beTRUSTed Lightweight Directory Access Protocol shadow to the local Land Information New Zealand directory.

6.5.5.1 External & Internal Firewall

A review of the firewall must be performed to ensure that only ports required to gain access to the **Landonline** Public Key Infrastructure and Registration Authority web site or communications between the web server and application server have been opened for incoming Public Key Infrastructure and Registration Authority traffic. Additionally, for out going traffic, only required ports must have been opened.

6.5.6 Operating and Management Procedures

Review the following technical activities to ensure they have been performed in accordance with documented procedures:

- Digital Certificate Registration;
- Digital Certificate Revocation;
- Routine Re-key;
- Digital Certificate Management for Registration Authority personnel;
- Directory Shadowing; and
- Audit Log Management.

6.6 Certificate Policy

All Digital Certificates that reference this policy shall be issued in the X.509 version 3 format and shall include a reference to this policy's Object Identifier within the appropriate field.

6.6.1 Certificate Policy Object Identifier

Digital Certificates issued under this policy shall have the Object Identifier as in section 1.2 Policy Identification.

7 DIGITAL CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES

7.1 Digital Certificate Profile

7.1.1 Version Number

The Certificate Authority must issue X.509 Version 3 Digital Certificates in accordance with Public-Key Infrastructure X.509 Part 1 Digital Certificate and Certificate Revocation List Profile.

Approved applications must support all the base (non-extension) X.509 fields:

Signature	: Certificate Authority signature for authentication
Issuer	: Name of Certificate Authority
Validity	: Commencement and expiry dates
Subject	: Subscriber's Distinguished Name
SubjectPublicKeyInformation	: algorithmID, key
Version	: Version of X.509 Digital Certificate, version 3
SerialNumber	: Unique serial number for Digital Certificate

7.1.2 Digital Certificate Extensions

All Entity Public Key Infrastructure software must correctly process the extensions identified in the Public-Key Infrastructure X.509 Digital Certificate profile.

The certificatePolicies extension must be used in all Digital Certificates and must be set as critical.

The PolicyIdentifier extension must contain the Object Identifier value.

7.1.3 Algorithm Object Identifiers

The Registration Authority personnel must use, and all entities must support, for signing and verification, the following algorithms:

- RSA 1024 or 2048 in accordance with PKCS#1 [10].
- SHA-1 in accordance with Federal Information Processing Standards PUB 180-1 [11] and American National Standards Institute X9.30 (Part 2) [12] - [ID sha1WithRSAEncryption, Object identifier 1 2 840 113549 1 1 5, Issuing Authority RSADSI].

All Entities may use, for signing and verification, the following algorithms:

- RSA 1024 in accordance with PKCS#1.

- SHA-1 in accordance with Federal Information Processing Standards PUB 180-1 and American National Standards Institute X9.30 (Part 2) - [ID sha1WithRSAEncryption, Object identifier 1 2 840 113549 1 1 5, Issuing Authority RSADSI].

7.1.4 Name Forms

Every Distinguished Name must be in the form of an X.501 printableString.

7.1.5 Name Constraints

The Distinguished Name in Subject and Issuer extension must comply with Public-Key Infrastructure X.509 Part 1 and be present in all Digital Certificates.

7.1.6 Certificate Policy Object Identifier

A Registration Authority personnel must ensure that the Policy Object Identifier is contained within the Digital Certificates it issues.

7.1.7 Usage of Policy Constraints Extension

The Registration Authority personnel must populate and mark as critical the policyConstraints extension.

7.1.8 Processing Semantics for the Critical Certificate Policy Extension

Critical extensions must be interpreted as defined in Public-Key Infrastructure X.509 part 1 [1].

7.2 Certificate Revocation List Profile

7.2.1 Version Number

The Certificate Authority must issue X.509 Version 2 Certificate Revocation Lists in accordance with Public-Key Infrastructure X.509 Part 1 Certificate and Certificate Revocation List Profile.

7.2.2 Certificate Revocation List and Certificate Revocation List Entry Extensions

All Entity Public Key Infrastructure software must correctly process all Certificate Revocation List extensions identified in the Public-Key Infrastructure X.509 Digital Certificate and Certificate Revocation List profile.

8 SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

8.1.1 Items that Can Change Without Notification

Changes to this policy which, in the judgement of the Land Information New Zealand, will not materially reduce the assurance that a Certificate Policy or its implementation provides, may be made without changing the Certificate Policy Object identifier and without notification to the Subscribers.

8.1.2 Changes With Notification

Prior to making any changes to this Certificate Policy, Land Information New Zealand will notify the Certificate Authority and all Subscribers of the changes. Any changes to a specification that amends the acceptability of Digital Certificates will require changes to this Certificate Policy's Object identifier.

8.1.3 Notification Mechanism

Land Information New Zealand will notify in writing to the Certificate Authority of any proposed changes to this Certificate Policy. The notification will contain a statement of proposed changes, the final date for receipt of comments and the proposed effective date of change.

Land Information New Zealand will also post a notice of the proposal on the *Landonline* web site.

8.1.4 Comment Period

The comment period will be thirty (30) days unless otherwise specified. The comment period will be defined in the change notification.

8.1.5 Mechanism to Handle Comments

Written and signed comments on proposed changes must be directed to the Registration Authority in consultation with beTRUSTed.

8.1.6 Period for Final Change Notice

The Registration Authority, in consultation with beTRUSTed, will determine the period of final change notice.

8.1.7 Items Whose Change Requires a New Policy

If a policy change is determined by the Registration Authority in consultation with beTRUSTed to warrant a new policy, beTRUSTed may assign a new Object Identifier to the modified policy and notify relevant parties of the change.

8.2 Publication and Notification Procedures

An electronic copy of this document is to be made available at :

- The Land Information New Zealand web site at www.landonline.govt.nz and
- Via an e-mail request to the Registration Authority at solutions@linz.govt.nz.

9 GLOSSARY

Activation data	The shared secret is the unique identifier provided by the Subscriber for authentication during Digital Certificate registration and creation. This is also called the “activation codes” or “shared secrets”.
Authority Revocation List (ARL)	A revocation list containing a list of public-key Digital Certificates issued to Certificate Authorities which are no longer considered valid by the Certificate Authority Digital Certificate issuer.
American National Standards Institute (ANSI)	American National Standards Institute is a voluntary organisation composed of over 1,300 members (including all the large computer companies) that creates standards for the computer industry.
beTRUSTed	The Certificate Authority selected by Land Information New Zealand to act as an outsourced Certificate Authority for the Landonline Public Key Infrastructure.
Certificate Authority (CA)	An entity trusted by one or more parties to issue and manage X.509 Digital Certificates, keys and Certificate Revocation Lists.
Certificate Policy (CP)	A statement derived from the Certification Practice Statement on an application by application basis, documenting specific additional conditions on any aspect of the certification process, including but not limited to identification and authentication, community and applicability. For any Digital Certificate, the applicable Certificate Policy is produced and published by the Registration Authority identified in the Digital Certificate.
Certificate Revocation List (CRL)	A list of revoked Digital Certificates that is created and signed by the same Certificate Authority that issued the Digital Certificates. A Digital Certificate is added to the list if it is revoked (e.g. because of suspected key compromise). In some circumstances the Certificate Authority may choose to split a Certificate Revocation List into a series of smaller pieces to improve search performance.
Certification Practice Statement (CPS)	A statement of the operational practices that the approved Certificate Authority in issuing, suspending, revoking and renewing Digital Certificates and providing access to such Digital Certificates.
Class 2 certificate	Class 2 certificates are issued to individuals. Class 2 certificates provide reasonable assurance of a subscriber's identity, based on a process that compares the applicant's personal information on the certificate application against the information contained in a government issued photo ID. Class 2 certificates are used in Landonline for users to connect through the external, web-based, interface and for signing transactions. Other classes of certificates have different proof of identity requirements and are not used by users of Landonline .
Common Name (CN)	The Common Name is the first part of the Distinguished Name string that defines the unique Subscriber name for each Subscriber under this branch of the Certificate Authority.
Digital Certificate	Digital Certificates issued by the approved Certificate Authority contain the Subscriber's public key. Landonline makes use of Subscriber Digital Certificates in authentication and signing validation (i.e. ensuring that the Subscriber is still a valid Subscriber at the time of signing, by not being listed on the Certificate Revocation List).
Distinguished Name (DN)	The Distinguished Name is used to provide a unique identity contained within a Subscriber's Digital Certificate. The Distinguished Name includes the Common Name as part of its string.
Federal Information Processing Standards (FIPS)	The Federal Information Processing Standards 140-1 level 2 validation list contains those crypto modules in security products that have been tested and validated under the Cryptographic Module Validation Program.

Internet Information Server (IIS)	Microsoft's web hosting solution package.
key pair	Two mathematically related asymmetric cryptographic keys (public and private), having the properties that (i) a message encrypted by either one of the keys can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Proof of Identity Certifier	Proof of Identity Certifiers are delegated responsibility from the Registration Authority to act in specific capacities around Subscriber registration and revocation administration. LINZ allows all named groups under the Oaths and Declarations Act 1957 to act as Proof of Identity Certifiers. Application for a digital certificate involves a proof of identity check. The Proof of Identity Certifiers certify the Subscriber's Government issued photo identification as a true copy.
Object identifier (OID)	A specially formatted number, registered with an internationally recognised standards Organisation, and associated with, for example, a class of Digital Certificates or a Certificate Policy.
private key	The un-revealed part of a key pair as used to create a public key or in Digital Signatures. Landonline Subscribers create their private key pair from their Internet browser during registration or re-key procedures.
private key archive	A copy of a private key made or used for any purpose other than as a disaster recovery back- up.
private key back-up	A copy of a valid, non-expired, private key held for disaster recovery purposes.
public key	The revealed part of a key pair, as used to verify a Digital Signature. The public keys are made freely available to Land Information New Zealand who shall receive digitally signed transactions from the Subscriber.
Pubic Key Cryptography Standard (PKCS)	The Pubic Key Cryptography Standard specifies a number of message and package formats. PKCS #12 provides a format for exchange of personal identity information.
Public Key Infrastructure (PKI)	A set of controls and standards governing the management of multiple Certification Authorities, to ensure recognition, availability and interoperability of Digital Certificates. The Public Key Infrastructure standards dictate how all entities and Digital Certificate procedures will work together.
Public-Key Infrastructure X.509 (PKIX)	Public-Key Infrastructure X.509 is the working group embarking on additional standards work to develop protocols that are either integral to Public Key Infrastructure management, or that are otherwise closely related to Public Key Infrastructure use.
Registration Authority (RA)	An entity that is delegated responsibility from the Certificate Authority to manage all Subscribers under that approved Certificate Authority. Managing Subscribers includes daily administration and audit log examination. The LINZ Proof of Identity Certifier will perform the "Proof of Identity" check on behalf of the Registration Authority.
Relying Party	Any entity that relies on or checks on the validity of Digital Certificates issued by the Certificate Authority. Land Information New Zealand is the only Relying Party on the use of Digital Certificates as described in this policy.
Request For Comment #2527 (RFC)	A document constructed by the network working group detailing Certificate Policy and Certification Practice Statement frameworks within the Internet X.509 Public Key Infrastructure. A Request for Comment itself is an Internet standard.
Rivest, Shamir, and Adelman (RSA)	A public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique. The RSA algorithm is based on the fact that there is no efficient way to factor very large numbers. Deducing an RSA key, therefore, requires an extraordinary

amount of computer processing power and time. The RSA algorithm has become the de facto standard for industrial-strength encryption, especially for data sent over the Internet.

Secure Hash Algorithm 1 (SHA-1)	A message digest algorithm designed and patented by RSA. A hash is a mathematical checksum calculated over a block of data to provide data integrity in such a way that if any one (1) bit of data is changed, the hash is changed. This is the basis of Digital Signature.
Secure Sockets Layer (SSL)	A protocol specified by Netscape that allows for "secure" passage of data. It uses public key encryption, including Digital Certificates and Digital Signatures, to pass data between an Internet browser and a server. It is an open standard and is supported by Netscape's Navigator and Microsoft's Internet Explorer.
Subscriber	The end user of the Certificate Authority issued individual Digital Certificate. This end user uses their Digital Certificate for Landonline purposes only and each Digital Certificate is unique to the Subscriber that owns it. Each Digital Certificate in Landonline is backed by a key pair in the Subscriber's Internet browser.
Trusted Contact	A specific role in Landonline where an individual at a firm or organisation bears certain obligations, as described in this Certificate Policy.
Trustworthy System	Applications, devices, and hardware, that, taken as a whole, provide a consistent audit trail of information which can be later be examined and trusted. Such records will be digitally signed or otherwise secured.
Uniform Resource Locator (URL)	The Uniform Resource Locator is the global address of documents and other resources on the World Wide Web.
X.509	The most widely used standard for defining Digital Certificates. X.509 is an International Telecommunication Union recommendation, which means that Public Key Infrastructure vendors do apply the standard in different ways. LINZ uses standard industry accepted X509 version three (3) (or v3) Digital Certificates as defined in this policy.