

THE NATIONAL BANK OF NEW ZEALAND  
Public Key Infrastructure (PKI)

Certificate Practice Statement

Certificate Policy (Subscriber)

Glossary

March 2005



# CERTIFICATION PRACTICE STATEMENT

---



**[www.nbnz.co.nz/pki](http://www.nbnz.co.nz/pki)**

**Object Identifier 1.2.36.5357522.5.2.5**

**Version 1.1**

**Date of issue: 09/03/2005**

**Date of Version 1.0 publication: March 2005**

**Date of Version 1.1 publication: April 2008**

# SUMMARY OF IMPORTANT RIGHTS AND OBLIGATIONS



This is a summary of important rights and obligations only. You must read this entire Certification Practice Statement, related Certificate Policy and Glossary, Subscriber Agreement and The National Bank Internet Product Terms to ensure you fully understand your rights and obligations in using The National Bank PKI.

1. This Certification Practice Statement controls the provision and use of The National Bank PKI service. All capitalised terms in this Certification Practice Statement are defined in the Glossary.
2. All Subscribers of The National Bank PKI services should, prior to applying for a Certificate, receive proper training in the use of public key technology and seek independent legal advice regarding their rights and obligations under this Certification Practice Statement, the relevant Certificate Policy, the Glossary, Subscriber Agreement and The National Bank Internet Product Terms.
3. A Key Pair (see Glossary) will be generated for all Certificate Holders and all Certificate Holders must keep the Private Key, Smart Card and pass-phrase secure.
4. All Certificates issued under The National Bank PKI can only be used for the limited purposes set out in the relevant Certificate Policy.
5. Subscribers are obliged to notify The National Bank upon compromise or suspected compromise of their Private Key and in certain other circumstances (see Subscriber Agreement).
6. Except as otherwise provided in the Subscriber Agreement, to the extent permitted by law, The National Bank excludes all warranties and The National Bank liability under the Subscriber Agreement, Certificate Policy and Certification Practice Statement is limited (see Subscriber Agreement).
7. Subscribers must provide certain indemnities to the Group (see Subscriber Agreement).
8. All Applicants and Certificate Holders will need to provide certain privacy consents regarding Personal Information they provide to The National Bank (see Section 2.4.2 of the Certification Practice Statement and the Subscriber Agreement).
9. The National Bank may in its absolute discretion terminate all services under The National Bank PKI on 10 Business Days notice to Subscribers (see Subscriber Agreement).

# TABLE OF CONTENTS



- CERTIFICATION PRACTICE STATEMENT ..... 2
- Summary of Important Rights and Obligations..... 3
- Table of Contents ..... 4
- 1. Introduction ..... 6
  - 1.1. Overview ..... 6
  - 1.2. Identification..... 6
  - 1.3. Community and Applicability..... 7
    - 1.3.1 Applicability ..... 10
  - 1.4. Contact Details within The National Bank ..... 10
- 2. General Provisions ..... 11
  - 2.1. Obligations ..... 11
    - 2.1.1 The National Bank’s obligations..... 11
    - 2.1.2 Subscriber obligations..... 11
    - 2.1.3 The National Bank Global Administrator obligations ..... 11
    - 2.1.4 Relying party obligations..... 11
  - 2.2. Publication, Repository and Notification Policies..... 11
    - 2.2.1 Access controls ..... 11
  - 2.3. Compliance Audit..... 12
  - 2.4. Confidentiality and Privacy ..... 12
    - 2.4.1 Types of information to be protected ..... 12
      - 2.4.1.1 Confidential Information..... 12
      - 2.4.1.2 Personal Information..... 12
    - 2.4.2 Intended uses and disclosures of Personal Information ..... 12
  - 2.5. Intellectual Property Rights..... 13
  - 2.6. Interpretation..... 13
- 3. Identification and Authentication ..... 14
  - 3.1. Initial Registration ..... 14
    - 3.1.1 Types of names..... 14
    - 3.1.2 Need for names to be meaningful..... 14
    - 3.1.3 Uniqueness of names ..... 14
    - 3.1.4 Name claim dispute resolution procedure..... 14
    - 3.1.5 Authentication of organisation and individual identity ..... 14
  - 3.2. Routine Certificate Renewal ..... 15
    - 3.2.1 Renewal ..... 15
    - 3.2.2 Renewal after Revocation..... 15
- 4. Operational Requirements ..... 16
  - 4.1. Certificate Application and Issuance ..... 16
  - 4.2. Certificate Acceptance..... 16
  - 4.3. Certificate Suspension and Revocation..... 16
  - 4.4. Circumstances for Suspension or Revocation..... 16
    - 4.4.1 Suspension of Revocation request ..... 17
    - 4.4.2 Who can request Suspension or Revocation..... 18
    - 4.4.3 Suspension or Revocation request grace period ..... 18
  - 4.5. Certificate Validity and Status Checks..... 18
  - 4.6. Cessation of Rights and Obligations ..... 18
  - 4.7. Security Audit Procedures ..... 19
  - 4.8. Records Archival..... 19



|                                       |  |    |
|---------------------------------------|--|----|
| 4.9.                                  | Compromise and Disaster Recovery .....                                   | 19 |
| 4.10.                                 | PKI Termination .....  | 19 |
| 5.                                    | Physical, Procedural, and Personnel Security Controls .....              | 20 |
| 5.1.                                  | Physical Controls .....  | 20 |
| 5.1.1                                 | The National Bank Security Policy .....                                  | 20 |
| 5.1.2                                 | Certification Authority site .....                                       | 20 |
| 5.2.                                  | Personnel Controls .....   | 20 |
| 5.2.1                                 | Background, qualifications, experience, and clearance requirements ..... | 20 |
| 5.2.2                                 | Training requirements and sanctions .....                                | 20 |
| 6.                                    | Technical Security Controls .....  | 21 |
| CERTIFICATION POLICY SUBSCRIBER ..... |  | 22 |
| Introduction .....                    |  | 23 |
| GLOSSARY .....                        |  | 25 |
| COPYRIGHT NOTICE .....                |  | 31 |

# 1. INTRODUCTION



## 1.1. Overview

### Acknowledgments

This Certification Practice Statement is based on the framework outlined in RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF, by S. Chokhani and W. Ford, The Internet Society, 1999.

### Certification Practice Statement

A Certification Practice Statement is a statement of the practices that a Certification Authority employs in issuing Certificates.

This Certification Practice Statement applies to one stream of the Public Key Infrastructure ('PKI') of The National Bank of New Zealand, part of ANZ National Bank Limited as agent for Australia and New Zealand Banking Group Limited ABN 11 005 357 522 ('The National Bank'). The common title of that stream is The National Bank of New Zealand Public Key Infrastructure ('The National Bank PKI').

The National Bank PKI governs the issuance and use of a Certificate and the associated Public Key. The Certificate allows a Subscriber secure access to The National Bank Internet Products.

### Certificate Policy

A Certificate Policy outlines policy on usage of Certificates by the persons to whom they are issued.

The relationship between a Certification Practice Statement and Certificate Policy.

A Certificate Policy states what assurance is placed in a Certificate. A Certification Practice Statement states how a Certification Authority establishes that assurance. In addition, the Certification Practice Statement applies only to a single Certification Authority and PKI stream, whereas several Certificate Policies may be issued under the PKI framework covering different usages.

## 1.2. Identification

Object Identifiers (OID) are globally unique identifiers, used to identify components within The National Bank PKI. OIDs allow parties using The National Bank PKI to identify and obtain from The National Bank the actual Certificate Policies and Certification Practice Statement applying to the use of that PKI Stream. The relevant OIDs are:

Certification Practice Statement 1.2.36.5357522.5.2.5

Certificate Policy (The National Bank Global Administrator) 1.2.36.5357522.5.2.2

Certificate Policy (Subscriber) 1.2.36.5357522.5.2.7

Glossary 1.2.36.5357522.5.2.8



### 1.3. Community and Applicability

#### **Role of The National Bank generally**

The National Bank will receive applications for, process and issue Certificates to Subscribers in accordance with this Certification Practice Statement and any other related documents.

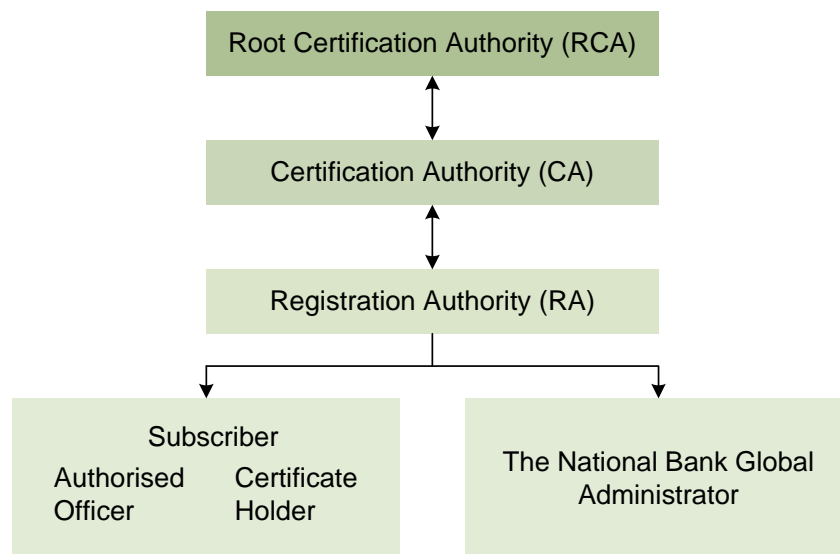
The operation of The National Bank PKI will be implemented in accordance with generally accepted security principles, covering computer hardware, software and procedures (including personnel practices) that:

- are appropriately secure from intrusion and misuse
- provide a reliable level of availability, reliability and correct operation
- are suited to performing their intended functions.

In addition to any other matter, The National Bank decides to consider in designing, implementing and maintaining a trustworthy PKI system, it will consider measures to:

- prevent unauthorised access to or use of the system, especially of Private Keys, and particularly a Certification Authority's Private Key used in issuing Certificates
- arrange personnel duties, access restrictions, and internal auditing procedures such that the system's security and operation cannot be compromised through the efforts of any single person having an interest in the outcome of system operations, or in collusion with other persons having an interest in the outcome of system operations
- provide contingency plans and processes designed to minimise consequences, should a primary security measure fail
- reduce the effects of natural disasters and any other events of Force Majeure, as well as the risk of financial difficulties, sabotage, employee fraud, and other foreseeable events
- maintain an auditable record of its services separately and independent of its operative system.

Among other things, The National Bank provides the Root Certification Authority, Certification Authority, Registration Authority and The National Bank Global Administrators under The National Bank PKI. The roles of these entities are outlined on the next page.



#### **Role of the Root Certification Authority**

The Root Certification Authority acts as the peak body for The National Bank PKI, establishes the chain of trust for Certificate issuance and issues Certificates to subordinate Certification Authorities.

#### **Role of Certification Authority**

The Certification Authority, which includes the system that automatically issues Certificates on receipt of a valid request from a subordinate Registration Authority, has the responsibility of ensuring The National Bank PKI is managed and operated within the Certification Practice Statement and associated Certificate Policies.

Under The National Bank PKI, the Certification Authority operates as follows:

- is subordinate to the Root Certification Authority
- is headed by a Certification Authority Officer ('CAO')
- administers the Certification Authority operation, issuing Certificates through a subordinate Registration Authority to Subscribers and to The National Bank Global Administrators
- is responsible for ensuring that it and any subordinate Registration Authority operates in accordance with relevant Certificate Policy, this Certification Practice Statement and other internal policy documents governing the Certification Authority and Registration Authority operations
- attends to Certificate Suspension or Revocation requirements, as advised by a Registration Authority
- is governed by the relevant Certificate Policies, such as:
  - PKI Certificate Policy (The National Bank Global Administrator)
  - PKI Certificate Policy (Subscriber).



### **Role of Registration Authority**

The Registration Authority, which includes the system that automatically processes Certificate requests received from a Subscriber or The National Bank Global Administrator(s), ensures all relevant requests comply with the Certification Practice Statement and associated Certificate Policies.

Under The National Bank PKI, all Registration Authorities operate as follows:

- are headed by a Registration Authority Officer ('RAO')
- are subordinate to the Certification Authority
- administer a Registration Authority operation, as part of the chain issuing Certificates to Subscribers and to The National Bank Global Administrators
- are responsible for monitoring that the Registration Authority and The National Bank Global Administrators operate in accordance with the relevant Certificate Policy, Certification Practice Statement and other internal policy documents governing Registration Authority operation and Certificate usage
- receive any Certificate Suspension or Revocation requests from Subscribers, and forward these to the Certification Authority Officer for actioning
- are governed by the relevant Certificate Policies, such as:
  - PKI Certificate Policy (The National Bank Global Administrator)
  - PKI Certificate Policy (Subscriber).

### **Role of The National Bank Global Administrators**

The National Bank Global Administrators:

- are responsible for administering individual system settings associated with Certificates to comply with Subscriber, The National Bank Internet Products and Certificate requirements and act as a contact point between The National Bank PKI and Subscribers
- manage the chain of trust between The National Bank and the Subscriber, are governed by the Certificate Policy (The National Bank Global Administrator) and this Certification Practice Statement
- process Certificate applications from Subscribers.

### **Role of Subscribers**

Subscribers use Certificates issued under The National Bank PKI to access The National Bank Internet Products. An Authorised Officer, nominated by a Subscriber, can also initiate Certificate requests on behalf of the Subscriber and within its business.

Under The National Bank PKI, the Subscribers operate as follows:

- have and maintain at least one Certificate Holder who is designated as an Authorised Officer, who has the authority to appoint further Authorised Officers
- receive a Certificate through the Registration Authority. An Authorised Officer of the Subscriber receives the initial Certificate, and is then able to initiate Certificate Issuance for other Certificate Holders



- use the Certificate to access the relevant National Bank Internet Products in line with the relevant Subscriber Agreement, Certificate Policy (Subscriber) and this Certification Practice Statement.

### **1.3.1 Applicability**

Certificates, issued under PKI, are used for identification purposes only, enabling a Subscriber access to National Bank Internet Products, and, as such, are referred to as Identity Certificates. These Certificates must only be used for the limited purposes set out in the relevant Certificate Policy and must not be used for any other purpose.

## **1.4. Contact Details within The National Bank**

Specific enquires regarding the usage of The National Bank PKI are to be directed, in the first instance, to the appropriate National Bank Internet Product Help Desk.

Other enquiries or communications about this document may be addressed to:

Manager, Business Security Management

The National Bank Trade Services

Level 2 ANZ House

Cnr Queen And Victoria Sts

Auckland 1001

email: [directtradeservices@nbnz.co.nz](mailto:directtradeservices@nbnz.co.nz)

## 2. GENERAL PROVISIONS



### 2.1. Obligations

#### 2.1.1 The National Bank's obligations

The National Bank's obligations in relation to the provision of a secure messaging infrastructure that enables the use of Keys and Certificates using Public Key cryptographic methods are set out in the Subscriber Agreement.

The Group's liability for any Loss a Subscriber incurs as a result of using that infrastructure will be limited under the relevant provisions of the Subscriber Agreement.

#### 2.1.2 Subscriber obligations

Subscriber (including Certificate Holder) obligations in relation to the use of The National Bank PKI are set out in the Subscriber Agreement, Certificate Policy (Subscriber) and this Certification Practice Statement.

Subscribers, (including Certificate Holders) must also comply with the relevant National Bank Internet Product Terms, which will be provided when Subscribers procure The National Bank's product or service that requires a PKI Certificate to be issued and used.

#### 2.1.3 The National Bank Global Administrator obligations

The rights and obligations of The National Bank Global Administrators in respect of their use of PKI are set out in the Certificate Policy (The National Bank Global Administrator).

#### 2.1.4 Relying party obligations

The National Bank and other members of the Group are the only relying parties under The National Bank PKI. The National Bank or the relevant members of the Group rely on Subscribers and Certificate Holders to comply with all the terms contained in the Subscriber Agreement, relevant Certificate Policy, this Certification Practice Statement and The National Bank Internet Product Terms.

### 2.2. Publication, Repository and Notification Policies

The Certification Authority website can be accessed via [www.nbnz.co.nz/pki](http://www.nbnz.co.nz/pki). This site includes a copy of relevant PKI documentation. These documents will be updated by the relevant CAO from time to time.

Any amendments to the Subscriber Agreement, the relevant Certificate Policy and this Certification Practice Statement will be made and notified to Subscribers, in accordance with the mechanism set out in the Subscriber Agreement.

#### 2.2.1 Access controls

The following access controls apply to the publication of documents on the website:

| Entity                          | Control                                     |
|---------------------------------|---|
| The National Bank               | Full maintenance rights.                    |
| Subscribers/Certificate Holders | Online access, with 'read only' permission. |
| Other parties or notices        | No access to publications.                  |



## **2.3. Compliance Audit**

The National Bank shall conduct detailed annual compliance audits of the practices of PKI. The first compliance audit will occur within the first 12 months of the commencement of operations of PKI.

## **2.4. Confidentiality and Privacy**

This section addresses the types of information that:

- must be kept confidential by The National Bank
- are not considered confidential
- collection, use and disclosure of personal information.

### **2.4.1 Types of information to be protected**

#### **2.4.1.1 Confidential Information**

Confidential Information is proprietary information of The National Bank or another party that The National Bank considers confidential or is deemed to be confidential by operation of contract or general law. The National Bank will take reasonable steps to protect any confidential information that it receives from other parties.

#### **2.4.1.2 Personal Information**

The Registration Information will contain Personal Information about Certificate Holders. The National Bank will ensure that the Registration Information will be collected, used, disclosed and held in accordance with the Privacy Act 1993 (NZ) and any other relevant legislation, the Subscriber Agreement and The National Bank Internet Product Terms.

The Subscriber acknowledges that The National Bank, in discharging its obligations under the Privacy Laws, is reliant on the Subscriber to ensure it provides Personal Information to The National Bank in a manner that complies with the Privacy Act 1993 (NZ) and any other relevant laws.

### **2.4.2 Intended uses and disclosures of Personal Information**

Certificate Holders agree to the use and disclosure of any Personal Information in the Certificate Information if:

- it is necessary in the ordinary course of The National Bank PKI operations;
- The National Bank receives a properly constituted warrant;
- The National Bank receives a court order or similar body having power to require production of that information or is otherwise compelled by law;
- the relevant Certificate Holder consents to the relevant disclosure or use or requests disclosure of that Personal Information to himself or herself;
- The National Bank needs to disclose Personal Information to third party service providers or allow them to collect or use such information for the purpose of operating, maintaining or enhancing PKI; or
- otherwise permitted under the Subscriber Agreement.



## 2.5. Intellectual Property Rights

This section addresses ownership rights of Certificates, practice and policy specifications, Distinguished Names, and Keys.

Unless otherwise agreed between The National Bank and a Subscriber:

- Intellectual Property rights ('IP rights') in The National Bank PKI, the Governing Documents, and any data or information generated or processed by PKI is owned by The National Bank or its licensors
- IP rights in Certificates and Key Pairs are owned by The National Bank, subject to any pre-existing IP rights, which may exist in the Certificates, the Certificate Information or the Key Pairs and are owned by other parties.

To the extent which the Subscriber owns any Intellectual Property rights in Certificate Information (including the common name field in the X.509 Distinguished Name) and any other matter provided by it or on its behalf ('Subscriber IP'), the Subscriber grants a non-revocable, perpetual, royalty-free, worldwide licence to The National Bank, and any other entity nominated by The National Bank, to use the Subscriber IP in any manner which is necessary or desirable for The National Bank or any other entity to operate, maintain or enhance The National Bank PKI at the date operations commence or at any time in the future.

The Subscriber warrants that:

- it has all the rights necessary to grant the licences described in this Section 2.5
- use by The National Bank or other entities of the relevant Subscriber IP in the manner contemplated by this Section 2.5 will not infringe the Intellectual Property rights of a third party.

The National Bank is not required to independently check, and will not independently check, the status of any trademark or other Intellectual Property rights that may subsist in any part of a Distinguished Name.

## 2.6. Interpretation

Unless otherwise defined in this Certification Practice Statement, words and phrases used in this Certification Practice Statement and defined in the Glossary, have the same meaning.

The provisions for interpretation and construction, severance, waiver and governing law contained in the Subscriber Agreement, also govern this Certification Practice Statement.

## 3. IDENTIFICATION AND AUTHENTICATION



### 3.1. Initial Registration

#### 3.1.1 Types of names

The National Bank assigns a Distinguished Name to each Authorised Officer or Applicant based on the Registration Information, in its absolute discretion.

The process to assign a Distinguished Name is to, initially, have the Registration Authority Officer (or other authorised individual) assign a Distinguished Name (except for the 'common name' element nominated by the Subscriber or Authorised Officer or Applicant) at the time a Certificate request is generated.

The Registration Authority then processes the request and passes it to the Certification Authority, which checks for the uniqueness of the Distinguished Name and whether the request conforms to this Certification Practice Statement, before generating a Certificate.

However, The National Bank may in its absolute discretion refuse to register or assign a Distinguished Name or any part of a Distinguished Name without providing reasons for doing so. If an Authorised Officer or Applicant is advised that its nominated Distinguished Name or any part of it has been rejected, it must choose another Distinguished Name. Examples of grounds on which The National Bank may reject a Distinguished Name include:

- obscene or offensive Distinguished Names
- where the Distinguished Name is likely to mislead or deceive
- where there are reasonable grounds for believing that a Distinguished Name infringes the Intellectual Property rights of any person
- where the use of a Distinguished Name would be contrary to law.

#### 3.1.2 Need for names to be meaningful

In addition to the restrictions set out in Section 3.1.1, Distinguished Names are only assigned if The National Bank considers in its absolute discretion that they are meaningful, ie. a name with commonly understood semantics allowing the identification of an individual or organisation that is the subject of the Certificate.

Anonymous names and pseudonyms (names other than the Certificate Holder's true name) will not be permitted to be registered.

#### 3.1.3 Uniqueness of names

Each Distinguished Name assigned will be unique in The National Bank PKI domain.

#### 3.1.4 Name claim dispute resolution procedure

If a dispute arises in relation to a Distinguished Name used by a Certificate Holder or Subscriber, The National Bank may in its absolute discretion and without liability to the Certificate Holder or Subscriber, suspend or revoke a Certificate because of such dispute.

#### 3.1.5 Authentication of organisation and individual identity

Any Evidence of Identity obligations, which arise in relation to a particular application for issue of a Certificate, will be performed in accordance with the relevant Certificate Policy.



## **3.2. Routine Certificate Renewal**

### **3.2.1 Renewal**

Certificate Holders are issued with new Keys and Certificates prior to, or on expiry of, their current Certificates without the requirement to re-check their identity and organisational status in the following circumstances:

- their current Certificates have not been revoked or suspended
- their Registration Information has not changed
- the Registration Authority which checked their identity and organisational status continues to operate without compromise
- a request for renewal is made by the Certificate Holder or relevant Subscriber prior to expiry of the Certificate Holder's current Certificate.

If all of these conditions are not satisfied, Certificate Holders applying for new Keys and Certificates on expiry of their current Certificate, must have their identity and organisational status verified in the same way as new applicants, as outlined under Section 3.1.5.

### **3.2.2 Renewal after Revocation**

In circumstances where renewal is required after Revocation, all conditions and procedures for issuance of a new Certificate must be met and followed.

## 4. OPERATIONAL REQUIREMENTS



This section outlines the specific requirements for the operational activities of The National Bank and Subscribers, which range from Certificate management to operational administrative functions such as audit, archive and business continuity planning.

### 4.1. Certificate Application and Issuance

A Certificate issuance request is accepted, following application and after all identification checks have been satisfactorily completed in accordance with the Facility Terms and the relevant National Bank Internet Product requirements.

Then the issuing process is:

- a Certificate issuance request is generated within The National Bank PKI systems
- a Certificate is created, if The National Bank determines that the request meets the requirements set out in this Certification Practice Statement
- The National Bank then securely delivers the Certificate to the Subscriber.

### 4.2. Certificate Acceptance

Any use of a Certificate after receipt constitutes the Subscriber's acceptance that the Certificate is duly created and complete, and the Registration Information provided is true and correct.

### 4.3. Certificate Suspension and Revocation

Certificate Suspension and/or Revocation are crucial to the maintenance of the integrity of The National Bank PKI.

The National Bank reserves the right to suspend or revoke Certificates. If The National Bank considers it, in its absolute discretion, to be prudent and practicable, it will advise the Subscriber of the proposed Suspension or Revocation, and give the Subscriber the opportunity to oppose the Suspension or Revocation unless the law provides otherwise.

If The National Bank using its best endeavours is unable to notify the Subscriber, then The National Bank can suspend or revoke the Certificate if it reasonably considers that the Suspension or Revocation is justified in the circumstances.

If, however, Suspension or Revocation of a Certificate is proven to be unjustified, new Certificates will be provided to the Subscriber at The National Bank's cost, but, otherwise, the liability of The National Bank and each member of the Group for any unjustifiable Revocation or Suspension is limited in accordance with the Subscriber Agreement.

### 4.4. Circumstances for Suspension or Revocation

The National Bank may suspend or revoke a Certificate:

- on receipt of a request to a National Bank Global Administrator or an Authorised Officer, from an authorised person (including Subscribers, Certificate Holders and other parties specified in section 4.4.2), subject to verification, in accordance with policies published from time to time
- if any of the following occurs:



- it is reasonably likely that the relevant Certificate has been compromised
- there are reasonable grounds for believing that the Subscriber has ceased trading or an Insolvency Event has occurred
- if The National Bank reasonably believes Certificate information has become inaccurate in a material respect
- any other change occurs that affects the accuracy and/or completeness of the Registration Information
- a lawful direction is received from an authorised third party e.g. a court order
- faulty or improper registration, Key generation or Certificate issuance has occurred
- a Certificate Holder ceases to be an employee or agent of the Subscriber
- the Subscriber or the Certificate Holder has not complied with any obligation under the Governing Documents
- if the Root Certification Authority Certificate has been suspended or revoked
- any other circumstances arise which The National Bank reasonably believes justifies Suspension or Revocation.
- The National Bank may, but is not required to, investigate any of the circumstances set out above.

If The National Bank does decide to investigate, then reasonable endeavours will be made to notify the Subscriber before the Certificate is suspended or revoked. In any case, The National Bank will take reasonable steps to notify a Certificate Holder as soon as practicable that its Certificate has been suspended or revoked. The National Bank's liability for unjustifiably revoking a Certificate is limited in the manner set out in Section 4.3.

#### 4.4.1 Suspension of Revocation request

The National Bank will verify that, (in accordance with policies it publishes from time to time), the party who has made a Suspension or Revocation request, is actually authorised to make such a request.

The following table displays acceptable forms of verification.

| Verification format | Verification process  |
|---------------------|---|
| In person           | Photo ID or any other verification information that The National Bank or its agents may request.        |
| Online              | Pass-phrase and/or any other verification information that The National Bank or its agents may request. |
| Telephone           | Pass-phrase and/or any other verification information that The National Bank or its agents may request. |



#### 4.4.2 Who can request Suspension or Revocation

The following persons or entities can request Suspension or Revocation:

| Person/Entity   | Suspension/Revocation action   |
|---|--|
| Certificate Holder  | Request The National Bank to suspend or revoke their Certificate at any time.  |
| Subscriber  | Request The National Bank to suspend or revoke a Certificate held by an Authorised Officer or Certificate Holder of that Subscriber.   |
| Authorised Officer  | Request The National Bank to suspend or revoke a Certificate issued by any Authorised Officer to a Certificate Holder.   |
| A person, nominated in the registration information, who certified or provided material evidence regarding the identity of the Subscriber or its personnel. | Request The National Bank to suspend or revoke a Certificate on the grounds that the Registration Information has changed.   |
| Any other person/entity (including by court order or direction)   | Request The National Bank to suspend or revoke a Certificate, providing The National Bank is satisfied that the Entity is lawfully; <ul style="list-style-type: none"><li>• empowered to do so</li><li>• entitled to administer the Subscriber's affairs, which relate to the Certificate</li><li>• its own, its employees, Officers or agents</li><li>• any Subscriber or Certificate Holder</li><li>• any Certification Authority or Registration Authority.</li></ul> |

#### 4.4.3 Suspension or Revocation request grace period

There is no grace period associated with a Suspension or Revocation request. Suspension and Revocation take effect immediately.

#### 4.5. Certificate Validity and Status Checks

The PKI relying systems will check the validity and status of a Certificate every time a Certificate is used to initiate a log on request, sign-on request or other appropriate security check in respect to The National Bank Internet Products.

#### 4.6. Cessation of Rights and Obligations

When a Certificate is suspended or revoked:

- then all rights associated with the Certificate cease
- the obligations associated with the Certificate will continue, to the extent that any of those obligations are capable of being fulfilled.



#### **4.7. Security Audit Procedures**

The National Bank will perform the following activities for the purpose of maintaining a secure environment within The National Bank PKI:

- record the following:
  - administrative activity (which includes changes to policies, Certificate Holder directories, pass-phrase policies) and other configuration changes
  - access and signing activity, which covers all activity by Certificate Holders including successful and failed logon attempts to The National Bank systems.
- moving audit logs to tape every day
- holding audit logs in archive for three months.

#### **4.8. Records Archival**

During the operation of The National Bank PKI, The National Bank records events, which it considers appropriate to assist in the security and reliability of that system.

Applicable New Zealand archive standards governing record retention are adhered to and archive media is protected using a combination of one or both physical and cryptographic protection.

#### **4.9. Compromise and Disaster Recovery**

The National Bank maintains a disaster recovery and business continuity plan covering reasonably foreseeable types of disasters and compromises including:

- Loss or corruption, including suspected corruption of computing resources, software or data.
- compromise of the Certification Authority Key or any other Private Key relied on to establish the chain of trust in Certificates.

The disaster recovery and business continuity plan used by The National Bank meets the requirements of appropriate Australian and New Zealand Standards ie. AS/NZS ISO/IEC 17799:2001.

#### **4.10. PKI Termination**

In the event The National Bank intends to terminate The National Bank PKI, Subscribers will be given a minimum of ten Business Day's written notice.

The Group will not be liable for any Losses any party incurs as a result of terminating The National Bank PKI operations under this Section. The National Bank may in its absolute discretion refund Subscribers a pro rata amount of any fees paid for the use of The National Bank PKI.

## 5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS



In addition to its general responsibilities regarding the maintenance of a secure PKI, set out in section 1.3, this section describes some of the non-technical controls The National Bank uses to provide a secure PKI.

### 5.1. Physical Controls

#### 5.1.1 The National Bank Security Policy

The National Bank maintains security policies outlining the protection required for Certification Authorities, in particular covering the areas of confidentiality, integrity and availability.

The National Bank security policies set out the rules all staff using any The National Bank information assets must comply with at all times.

#### 5.1.2 Certification Authority site

The Certification Authority is housed within a restricted access computer room within a secure data centre.

Access to the data centre is restricted and it is protected from power outages, fire and water exposure. All information generated, processed or held by the Certification Authority is protected in accordance with generally accepted industry standards.

### 5.2. Personnel Controls

#### 5.2.1 Background, qualifications, experience, and clearance requirements

The Group employs personnel and management practices to promote the trustworthiness, integrity and professional conduct of its staff. The selection of staff takes into consideration technical and business background, qualifications and experience for each role.

#### 5.2.2 Training requirements and sanctions

The National Bank PKI operations staff receive initial and continuing training, which is appropriate to the task and role a staff member performs. All Group staff are bound by internal policies which include sanctions for unauthorised actions.

## 6. TECHNICAL SECURITY CONTROLS



The National Bank maintains policies and procedures outlining the security measures taken in relation to its general responsibilities regarding the maintenance of a secure PKI, including protection of Certificates and cryptographic system data.

# CERTIFICATION POLICY SUBSCRIBER

---



**[www.nbnz.co.nz/pki](http://www.nbnz.co.nz/pki)**

**Version 1.0**

**Object Identifier: 1.2.36.5357522.5.2.7**

**Date of issue: 09/03/2005**

**Date of Version 1.0 publication: March 2005**

**Date of Version 1.1 publication: April 2008**



## 1. CERTIFICATES – PERMITTED USES

- 1.1 This Certificate Policy is the principal statement of policy governing the permitted uses and Validity Period of Certificates issued to personnel nominated by Subscribers under The National Bank PKI.
- 1.2 Subscriber Certificates are administered by The National Bank and issued:
  - (1) to nominated personnel of Subscribers, where the Subscriber has entered into a Subscriber Agreement with a member of the Group and who agree to be bound by the Certificate Practice Statement
  - (2) solely for use by such personnel to:
    - (a) authenticate themselves to The National Bank
    - (b) confidentially access The National Bank Internet Products
    - (c) initiate certain instructions to a member of the Group
    - (d) communicate with The National Bank and are not to be used for any other purpose.
- 1.3 For the sake of certainty, the issuance of a Certificate does not in itself permit a Certificate Holder to access or use any National Bank Internet Product. Authorisation for such activities will have to be independently obtained from The National Bank for each relevant National Bank Internet Product (for example, by agreeing to be bound by the relevant National Bank Internet Product Terms).
- 1.4 Certificates must not in any circumstances be used for any other purpose other than those set out in this clause and The National Bank expressly disclaims all such unauthorised use, and any liability arising out of such other uses.

## 2. VALIDITY PERIOD

- 2.1 The Validity Period of a Certificate issued under this Certificate Policy will be two years.

## 3. RELATIONSHIP TO THE CERTIFICATION PRACTICE STATEMENT AND OTHER DOCUMENTS

- 3.1 This Certificate Policy documents the permitted uses and Validity Period of Subscriber Certificates under The National Bank PKI. The Certification Practice Statement details:
  - (1) the actual steps The National Bank takes in issuing Certificates and operating The National Bank PKI
  - (2) other rights and obligations that Subscribers and Certificate Holders have under PKI
  - (3) The National Bank also uses a Subscriber Agreement to ensure Subscribers and Certificate Holders perform certain obligations to ensure the overall security of The National Bank PKI is maintained.
- 3.2 This Certificate Policy must be read in conjunction with the associated Certification Practice Statement and the related Subscriber Agreement for The National Bank PKI.



3.3 Unless otherwise defined in this Certificate Policy, words and phrases used in this Certificate Policy and defined in the Glossary, have the same meaning. The provisions in respect of construction and general interpretation contained in the Subscriber Agreement apply to this Certificate Policy and are deemed incorporated in this Certificate Policy.

#### **4. AUDIENCE**

4.1 This Certificate Policy is only intended to be referred to by those persons who propose to subscribe or have subscribed to The National Bank PKI.

#### **5. EVIDENCE OF IDENTITY**

5.1 The PKI issues Certificates to Subscribers and Certificate Holders for the purposes of granting access to The National Bank Internet Products. In this context, the party relying on the Certificate is The National Bank or some other member of the Group, and in particular the business division responsible for the relevant National Bank Internet Products ('Business Division').

The Business Divisions have responsibility for ensuring that only authorised and known parties are able to access and use any National Bank Internet Products using Certificates, and will determine and perform the requisite level of Evidence of Identity ('EOI') checking required for such activities. In some cases the responsibility for performance of these checks may be the responsibility of the Subscriber, which will perform the EOI checks in accordance with any agreement with The National Bank.

The National Bank will maintain any information collected by the Business Divisions for the purposes of EOI in accordance with the Financial Transactions Reporting Act 1996 (NZ) and any other relevant legislation.

# GLOSSARY

---



**[www.nbnz.co.nz/pki](http://www.nbnz.co.nz/pki)**

**Version 1.0**

**Object Identifier: 1.2.36.5357522.5.2.8**

**Date of issue: 09/03/2005**

**Date of Version 1.0 publication: March 2005**

**Date of Version 1.1 publication: April 2008**



**'Applicant'** means an individual nominated by an Authorised Officer of the Subscriber as a person in favour of whom a Certificate may be issued.

**'Authorised Officer'** means a director or secretary of the Subscriber, or any other person appointed in writing, from time to time, by the Subscriber, to act as an authorised Officer who will be responsible for ensuring that the issuance and use of Certificates he or she is responsible for complies with the terms contained in the Governing Documents.

**'Business Day'** means a day that is not a Saturday, a Sunday, a public holiday or a regional holiday in New Zealand.

**'CAO'** see Certification Authority Officer.

**'Certificate'** means a secure token based record that:

- (a) identifies the issuer, which is the Root Certification Authority in the case of a Certificate issued to the Certificate Authority and the Certificate Authority in the case of Certificates issued to either a Registration Authority or a Certificate Holder;
- (b) names or identifies a Certificate Holder;
- (c) contains the Public Key of the Certificate Holder;
- (d) contains the name of the Subscriber on whose behalf the Certificate was issued;
- (e) identifies the Certificate's Validity Period;
- (f) is digitally signed by the issuer; and
- (g) is used in conjunction with the corresponding Private Key whenever the Certificate Holder creates a Digital Signature in order to authenticate the holder to The National Bank.

A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.

**'Certificate Holder'** means an individual nominated by or on behalf of the Subscriber who is named or identified in a Certificate issued in respect of that Subscriber.

**'Certificate Information'** means information needed to complete a Certificate as required by the Certificate Profile and includes some or all of the Registration Information.

**'Certificate Policy'** means a document being a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.

**'Certificate Policy (The National Bank Global Administrator)'** means a document being The National Bank PKI Certificate Policy (The National Bank Global Administrator), as amended from time to time, applicable to The National Bank Global Administrators.

**'Certificate Policy (Subscriber)'** means a document being The National Bank PKI Certificate Policy (Subscriber), as amended from time to time, applicable to Subscribers.

**'Certification Authority'** means the entity including the system that automatically issues Certificates on receipt of a valid request from a subordinate Registration Authority, that has the responsibility of



ensuring The National Bank PKI is managed and operated within the Certification Practice Statement and associated Certificate Policies.

**'Certification Authority Officer'** means a person who is responsible for ensuring the proper maintenance and support of a Certification Authority.

**'Certification Practice Statement'** means a document, as amended from time to time, that describes the practices to be performed under The National Bank PKI.

**'Confidential Information'** means all proprietary information of every kind concerning or any way connected with The National Bank PKI.

**'Digital Certificate'** see Certificate.

**'Digital Signature'** means the transformation of an electronic record by one person using a Private Key and Public Key cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine:

- (a) whether the transformation was created using the Private Key that corresponds to the Public Key; and
- (b) whether the record has been altered since the transformation was made.

**'Distinguished Name'** means a unique identifier assigned to each Certificate Holder, having the structure required by the Certificate Profile.

**'EOI'** see Evidence of Identity.

**'Evidence of Identity'** means establishment of the identity of an individual or an entity, and that the individual is authorised to represent an entity.

**'Facility'** means The National Bank's facility whereby it can issue Certificates to individuals to enable those persons to identify themselves and the entities they represent to various National Bank Internet Products offered by the Group and thus allow authenticated access to those systems.

**'Facility Terms'** means the Subscriber Agreement, the relevant Certificate Policy, the Certification Practice Statement and this Glossary.

**'Fee Schedule'** means the schedule from time to time published by The National Bank setting out the fees applicable to the issuance, use, cancellation, suspension and revocation of Certificates, and the creation, operation and termination of the Facility.

**'Fees'** means the fees specified in the Fee Schedule.

**'Force Majeure'** means any act of god, war, revolution, terrorist act or other unlawful act against public order or authority, an industrial dispute, a governmental restraint or any other event or cause which is not within the reasonable control of The National Bank.

**'Glossary'** means this document.

**'Governing Documents'** means the Certification Practice Statement, relevant Certificate Policies, Subscriber Agreement, this Glossary and National Bank Internet Product Terms.

**'Group'** means Australia and New Zealand Banking Group Limited ABN 11 005 357 522 and all related companies including:



- (1) all related bodies corporate (within the meaning of section 9 of the Corporations Act 2001 (Australia));
- (2) ANZ National Bank Limited within the meaning of section 2(5) of the Companies Act 1993 (NZ).

**'Insolvency Event'** means in respect of a person that:

- (a) the person is unable to pay its debts as they fall due;
- (b) the person has a receiver, receiver and manager, mortgagee in possession or voluntary administrator appointed to it or any of its assets or a decision or steps are taken to make any such appointment;
- (c) the person becomes subject to statutory management or to any other form of external administration;
- (d) a resolution is passed for the person's winding up or an order is made for the person's winding up;
- (e) an application for the person's winding up is presented, which relates to an amount of money owed by the person which is not bona fide in dispute;
- (f) in the case of a partnership, the partnership is dissolved; or
- (g) in the case of a natural person, the person dies or becomes bankrupt.

**'Intellectual Property'** means copyright and neighbouring rights, all rights in relation to inventions (including patent rights), registered and unregistered trademarks (including service marks), registered designs, confidential information (including trade secrets and know how), databases, and circuit layouts, and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.

**'Key'** means a sequence of symbols that control the operation of a cryptographic transformation.

**'Key Pair'** means a pair of Keys consisting of a Public Key and a Private Key.

**'Loss/Losses'** means any loss, damage, cost, interest, expense, fee, penalty, fine, forfeiture, assessment, demand, action, suit, claim, proceeding, cause of action, liability or damages incurred by a person, and includes:

- (a) the cost of any action taken by the person to protect itself against any loss or to preserve any right it has under the Facility Terms;
- (b) any taxes or duties payable in connection with the Facility Terms (other than tax on assessable income); and
- (c) where applicable, legal costs on an indemnity basis or on a solicitor and own client basis, whichever is higher.

**'Personal Information'** has the same meaning as in section 2 of the Privacy Act 1993 (NZ), namely information about an identifiable individual, and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995, or any former Act.

**'PKI'** see Public Key Infrastructure.

**'Private Key'** means the Private Key used by a Certificate Holder to digitally sign messages on behalf of a Subscriber.



**'Public Key'** means the Public Key (contained in a Certificate together with other information) corresponding to a Private Key, used to authenticate a Digital Signature.

**'Public Key Infrastructure'** means the combination of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke Public Key Certificates based on public key cryptography.

**'RAO'** see Registration Authority Officer.

**'Registration Authority'** means the system that automatically processes Certificate requests received from a Subscriber or The National Bank Global Administrator(s), and ensures all relevant requests comply with the Certification Practice Statement and associated Certificate Policies.

**'Registration Authority Officer'** means a person who is responsible for ensuring the proper maintenance and support of a Registration Authority and its functions.

**'Registration Information'** means the information Subscribers and Applicants must provide in order to apply for a Certificate, including any Personal Information.

**'Representative'** of a party means that party's director, Officer or employee.

**'Revocation/Revoke'** means to permanently terminate the Validity Period of a Certificate.

**'Root Certification Authority'** means the peak body for The National Bank PKI. It establishes the chain of trust for Certificate issuance and issues Certificates to subordinate Certification Authorities.

**'Secure Token'** means a physical device such as a smart card with computer processing capabilities used to securely generate Keys for a Certificate Holder.

**'Subscriber'** means a Subscriber that uses (through nominated personnel) Certificates issued under PKI to access any National Bank Internet Products.

**'Subscriber Agreement'** means an agreement between The National Bank and a Subscriber, which together with the Certification Practice Statement and relevant Certificate Policy governs the application for issuance and use of Certificates and The National Bank PKI.

**'Suspension/Suspend'** means to temporarily suspend the Validity Period of a Certificate for a specified time period.

**'The National Bank'** means The National Bank of New Zealand, part of ANZ National Bank Limited, with its registered office in Wellington, New Zealand as agent for Australia and New Zealand Banking Group Limited ABN 11 005 357 522.

**'The National Bank Global Administrator'** means a person responsible for administering individual system settings to comply with Subscriber, product and Certificate requirements.

**'The National Bank Internet Products'** means any National Bank Internet based product that uses The National Bank PKI.

**'The National Bank Internet Product Terms'** means the terms and conditions contained in any agreement a Subscriber (or Authorised Officer or Certificate Holder on behalf of a Subscriber) enters into relating to the use of The National Bank Internet Products.

**'The National Bank PKI'** or **'Public Key Infrastructure'** (also known as 'External', 'External PKI', or 'External Public Key Infrastructure') means PKI designed to accommodate Certificate issuance covering The National Bank customer access to The National Bank Internet Products.



**'Technology'** means the relevant computer software, Secure Token (including the Certificate and any application/software stored on the device) and reader (if any) to be provided to the Subscriber by The National Bank.

**'Validity Period'** means the period within which a Certificate can be validly used under The National Bank PKI, being the period stipulated in each Certificate and as varied by Suspension or Revocation performed in accordance with the Certification Practice Statement.

# COPYRIGHT NOTICE



© Australia and New Zealand Banking Group Limited ABN 11 005 357 522 is the owner of copyright in this document made/published in Australia in March 2005.

This document may be copied and provided to others provided that the reason it is copied and provided to others is directly related to the use of The National Bank PKI, and so long as the entire document is copied in its original form and remains unaltered in any way.

These terms and conditions are current as at 1 March 2005. The National Bank of New Zealand, part of ANZ National Bank Limited.

NBU 7244

04/08

