ANZ PKI

Australia

Certification Practice Statement
Certificate Policy (Subscriber)
Glossary

September 2002

Certification Practice Statement

Date of publication: September 2002

Version 2

Australia and New Zealand Banking Group Limited ABN 11 005 357 522

www.anz.com/pki

Object Identifier 1.2.36.5357522.5.2.1

Version 2.0

Date of issue 10/09/2002

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 ANZ Group Internet Products Terms to ensure you fully understand your rights and obligations in using ANZ PKI.

1. This Certification Practice Statement controls the provision and use of ANZ PKI service. All capitalised terms in this Certification Practice Statement are defined in the Glossary.
2. All Subscribers of ANZ 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 ANZ Group Internet Products 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 ANZ PKI can only be used for the limited purposes set out in the relevant Certificate Policy.
5. Subscribers are obliged to notify ANZ 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, ANZ excludes all warranties and ANZ's liability under the Subscriber Agreement, Certificate Policy and Certification Practice Statement is limited (see Subscriber Agreement).
7. Subscribers must provide certain indemnities to the ANZ Group (see Subscriber Agreement).
8. All Applicants and Certificate Holders will need to provide certain privacy consents regarding Personal Information they provide to ANZ (see Section 2.4.2 of the Certification Practice Statement and the Subscriber Agreement).
9. ANZ may in its absolute discretion terminate all services under ANZ PKI on 10 Business Days notice to Subscribers (see Subscriber Agreement).

Table of Contents

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 Australia and New Zealand Banking Group Limited (ANZ). The common title of that stream is the ANZ Public Key Infrastructure (**"ANZ PKI"**).

The ANZ PKI governs the issuance and use of a Certificate and the associated Public Key. The Certificate allows a Subscriber secure access to ANZ Group 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 ANZ PKI. OIDs allow parties using ANZ PKI to identify and obtain from ANZ the actual Certificate Policies and Certification Practice Statement applying to the use of that PKI Stream. The relevant OIDs are:

Certification Practice Statement
1.2.36.5357522.5.2.1

Certificate Policy (ANZ Global Administrator)
1.2.36.5357522.5.2.2

Certificate Policy (Subscriber)
1.2.36.5357522.5.2.3

Glossary
1.2.36.5357522.5.2.4

1.3 Community and Applicability

Role of ANZ generally

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

- are 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, ANZ decides to consider in designing, implementing and maintaining a trustworthy ANZ 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, ANZ provides an ANZ Root Certification Authority, Certification Authority, Registration Authority and ANZ Global Administrators under the ANZ PKI. The roles of these entities are outlined on the next page.

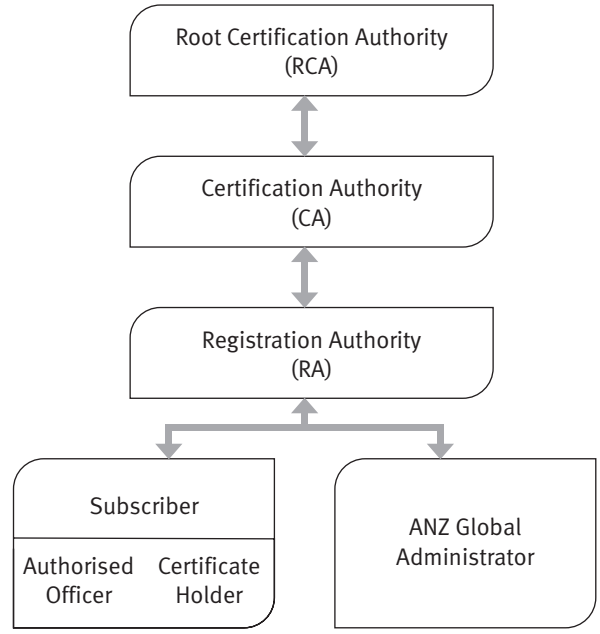

Figure 1 ANZ PKI Chain of Trust

Role of ANZ Root Certification Authority

The ANZ Root Certification Authority acts as the peak body for ANZ 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 ANZ PKI is managed and operated within the Certification Practice Statement and associated Certificate Policies.

Under ANZ PKI, the Certification Authority operates as follows:

- is subordinate to the ANZ 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 ANZ 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:
  – ANZ PKI Certificate Policy (ANZ Global Administrator)
  – ANZ 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 ANZ Global Administrator(s), ensures all relevant requests comply with the Certification Practice Statement and associated Certificate Policies.

Under ANZ 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 ANZ Global Administrators
› are responsible for ensuring the Registration Authority, Subscribers and the ANZ 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:
  – ANZ PKI Certificate Policy (ANZ Global Administrator)
  – ANZ PKI Certificate Policy (Subscriber).

Role of ANZ Global Administrators

ANZ Global Administrators:

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

Role of Subscribers

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

Under ANZ 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 relevant ANZ Group Internet Products in line with the relevant Subscriber Agreement, Certificate Policy (Subscriber) and this Certification Practice Statement.

1.3.1 Applicability

Certificates, issued under ANZ PKI, are used for identification purposes only, enabling a Subscriber access to ANZ Group 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 ANZ

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

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

Manager, Business Security Management
Group Information Security
ANZ Banking Group Limited
12/100 Queen Street
Melbourne VIC 3000
Australia.

2. General Provisions

2.1 Obligations

2.1.1 ANZ obligations

ANZ'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.

ANZ 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 ANZ 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 ANZ Group Internet Products Terms, which will be provided when Subscribers procure the ANZ Group product or service that requires an ANZ PKI Certificate to be issued and used.

2.1.3 ANZ Global Administrator obligations

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

2.1.4 Relying party obligations

ANZ and other members of the ANZ Group are the only relying parties under ANZ PKI. ANZ or the relevant members of the ANZ 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 ANZ Group Internet Products Terms.

2.2 Publication, Repository and Notification Policies

The Certification Authority website can be accessed via www.anz.com/pki. This site includes a copy of relevant ANZ 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**
ANZ	Full maintenance rights.
Subscribers/Certificate Holders	Online access, with 'read only' permission.
Other parties	No access to publications or notices.

2.3 Compliance Audit

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

2.4 Confidentiality and Privacy

This section addresses the:

- types of information that:
  - must be kept confidential by ANZ
  - 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 ANZ or another party that ANZ considers confidential or is deemed to be confidential by operation of contract or general law. ANZ 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. ANZ will ensure that the Registration Information will be collected, used, disclosed and held in accordance with the *Privacy Act 1988 (Cth)*, the Subscriber Agreement and ANZ Group Internet Products Terms.

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 ANZ PKI operations
- ANZ receives a properly constituted warrant
- ANZ receives a court order or similar body having power to require production of that information or is otherwise compelled by law
- the relevant individual requests disclosure
- ANZ 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 ANZ PKI
- 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 ANZ and a Subscriber:

- Intellectual Property rights (**"IP rights"**) in ANZ PKI the Governing Documents, and any data or information generated or processed by ANZ PKI is owned by ANZ or its licensors
- IP rights in Certificates and Key Pairs are owned by ANZ, 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 ANZ, and any other entity nominated by ANZ, to use the Subscriber IP in any manner which is necessary or desirable for ANZ or any other entity to operate, maintain or enhance ANZ 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 ANZ 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.

ANZ 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

ANZ assigns a Distinguished Name to each 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 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, ANZ 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 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 ANZ 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 ANZ 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 ANZ 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, ANZ 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 ANZ 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 relevant ANZ Group Internet Product requirements.

Then the issuing process is:

- a Certificate issuance request is generated within ANZ PKI systems
- a Certificate is created, if ANZ determines that the request meets the requirements set out in this Certification Practice Statement
- the ANZ 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 ANZ PKI.

The ANZ reserves the right to suspend or revoke Certificates. If ANZ 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 ANZ using its best endeavours is unable to notify the Subscriber, then the ANZ 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 ANZ's cost, but, otherwise, the liability of ANZ and each member of the ANZ Group for any unjustifiable Revocation or Suspension is limited in accordance with the Subscriber Agreement.

4.4 Circumstances for Suspension or Revocation

ANZ may suspend or revoke a Certificate:

- on receipt of a request to an ANZ 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 ANZ 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 eg. 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 ANZ Root Certification Authority Certificate has been suspended or revoked
  - any other circumstances arise which ANZ reasonably believes justifies Suspension or Revocation.

ANZ may, but is not required to, investigate any of the circumstances set out above. If ANZ does decide to investigate, then reasonable endeavours will be made to notify the Subscriber before the Certificate is suspended or revoked. In any case, ANZ will take reasonable steps to notify a Certificate Holder as soon as practicable that its Certificate has been suspended or revoked. ANZ'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

ANZ 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 ANZ or its agents may request.
Online	Pass-phrase and/or any other verification information that ANZ or its agents may request.
Telephone	Pass-phrase and/or any other verification information that ANZ 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 ANZ to suspend or revoke their Certificate at any time.
Subscriber	Request ANZ to suspend or revoke a Certificate held by an Authorised Officer or Certificate Holder of that Subscriber.
Authorised Officer	Request ANZ 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 ANZ 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 ANZ to suspend or revoke a Certificate, providing ANZ is satisfied that the Entity is lawfully: › empowered to do so › entitled to administer the Subscriber's affairs, which relate to the Certificate.
ANZ	Suspend or revoke a Certificate of: › its own, its employees, officers or agents › any Subscriber or Certificate Holder › any Certification Authority or Registration Authority.

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 ANZ PKI relying systems will check the validity and status of a Certificate every time a Certificate is used to initiate a logon request, sign-on request or other appropriate security check in respect to the ANZ Group 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

ANZ will perform the following activities for the purpose of maintaining a secure environment within the ANZ 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 ANZ systems.
- moving audit logs to tape every day
- holding audit logs in archive for three months.

4.8 Records Archival

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

Applicable Australian 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

ANZ 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 ANZ meets the requirements of appropriate Australian and New Zealand Standards ie. AS/NZS ISO/IEC 17799: 2001.

4.10 ANZ PKI Termination

In the event ANZ intends to terminate the ANZ PKI, Subscribers will be given a minimum of 10 Business Days written notice.

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

5. Physical, Procedural, and Personnel Security Controls

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

5.1 Physical Controls

5.1.1 ANZ Security Policy

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

ANZ security policies set out the rules all staff using any ANZ 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

ANZ 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

ANZ PKI operations staff receive initial and continuing training, which is appropriate to the task and role a staff member performs.

All ANZ Group staff are bound by internal policies which include sanctions for unauthorised actions.

6. Technical Security Controls

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

Certificate Policy (Subscriber)

www.anz.com/pki
Object Identifier 1.2.36.5357522.5.2.3
Version 2.0
Date of issue 10/09/2002

Introduction

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 ANZ PKI.

1.2 Subscriber Certificates are administered by ANZ and issued:

(1) to nominated personnel of Subscribers, where the Subscriber has entered into a Subscriber Agreement with a member of the ANZ Group and who agree to be bound by the Certificate Practice Statement

(2) solely for use by such personnel to:

(a) authenticate themselves to ANZ

(b) confidentially access ANZ Group Internet Products

(c) initiate certain instructions to a member of ANZ Group

(d) communicate with ANZ

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 ANZ Group Internet Product. Authorisation for such activities will have to be independently obtained from ANZ for each relevant ANZ Group Internet Product (for example, by agreeing to be bound by the relevant ANZ Group Internet Products Terms).

1.4 Certificates must not in any circumstances be used for any other purpose other than those set out in this clause and ANZ 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 2 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 ANZ PKI. The Certification Practice Statement details:

(1) the actual steps the ANZ takes in issuing Certificates and operating the ANZ PKI

(2) other rights and obligations that Subscribers and Certificate Holders have under ANZ PKI.

3.2 The ANZ also uses a Subscriber Agreement to ensure Subscribers and Certificate Holders perform certain obligations to ensure the overall security of the ANZ PKI is maintained.

3.3 This Certificate Policy must be read in conjunction with the associated Certification Practice Statement and the related Subscriber Agreement for ANZ PKI.

3.4 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 ANZ PKI.

5. Evidence of Identity

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

The Business Divisions have responsibility for ensuring that only authorised and known parties are able to access and use any ANZ Group 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 ANZ.

5.2 ANZ will maintain any information collected by the Business Divisions for the purposes of EOI in accordance with the *Financial Transaction Reports Act 1988 (Cth)*.

Glossary

www.anz.com/pki
Object Identifier 1.2.36.5357522.5.2.4
Version 2.0
Date of issue 10/09/2002

"ANZ" means the Australia and New Zealand Banking Group Limited ABN 11 005 357 522.

"ANZ Global Administrator" means a person responsible for administering individual system settings to comply with Subscriber, product and Certificate requirements.

"ANZ Group" means the Australia and New Zealand Banking Group Limited ABN 11 005 357 522 and all related bodies corporate (within the meaning of section 9 of the Corporations Act 2001).

"ANZ Group Internet Products" means any ANZ Group Internet based product that uses ANZ PKI.

"ANZ Group Internet Products 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 ANZ Group Internet Products.

"ANZ PKI" or **"ANZ Public Key Infrastructure"** (also known as "ANZ External", "ANZ External PKI", or "ANZ External Public Key Infrastructure") means PKI designed to accommodate certificate issuance covering ANZ customer access to ANZ Group Internet Products.

"ANZ Root Certification Authority" means the peak body for ANZ PKI. It establishes the chain of trust for Certificate issuance and issues Certificates to subordinate Certification Authorities.

"Applicants" 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 to the terms contained in the Governing Documents.

"Business Day" means a day that is not a Saturday, a Sunday, a public holiday or a bank holiday in the State of Victoria.

"CAO" *see Certification Authority Officer.*

"Certificate" means a secure token based record that:

(a) identifies the issuer, which is the ANZ 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) identifies the Certificate's Validity Period;
(e) is digitally signed by the issuer; and
(f) is used in conjunction with the corresponding Private Key whenever the Certificate Holder creates a Digital Signature in order to authenticate the holder to ANZ.

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 (ANZ Global Administrator)" means a document being the ANZ PKI Certificate Policy (ANZ Global Administrator), as amended from time to time, applicable to ANZ Global Administrators.

"Certificate Policy (Subscriber)" means a document being the ANZ 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 ANZ 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 ANZ PKI.

"Confidential Information" means all proprietary information of every kind concerning or any way connected with the ANZ 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 ANZ's facility whereby it can issue digital certificates to individuals to enable those persons to identify themselves and the entities they represent to various ANZ Group Internet Products offered by the ANZ 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 ANZ 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 ANZ.

"Glossary" means this document.

"Governing Documents" means the Certification Practice Statement, relevant Certificate Policies, Subscriber Agreement, this Glossary and ANZ Group Internet Products Terms.

"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 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 its 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 6 of the *Privacy Act 1988 (Cth)*, namely information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

"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 ANZ Global Administrator(s), 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.

"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 ANZ PKI to access any ANZ Group Internet Products.

"Subscriber Agreement" means an agreement between ANZ and a Subscriber, which together with this Certification Practice Statement and relevant Certificate Policy governs the application for issuance and use of Certificates and ANZ PKI.

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

"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 ANZ.

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

Item No. 77796 Version 2 W25744 09.2002

www.anz.com