CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

ANZ

CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

APPLICATION OF THIS DOCUMENT

The ANZ Certificate Policy **(Subscriber) (Certificate Policy (Subscriber))** in Part A must be read in conjunction with the ANZ Certification Practice Statement **(CPS)** in Part B.

Any capitalised terms which are not defined in the body of this document are defined in the Glossary (Part C).

The Certificate Policy (Subscriber) is the principal statement of policy governing the permitted uses and Validity Period of Digital Certificates issued to personnel nominated by You **(Users)**.

The CPS is a statement of the practices that a Certification Authority employs in issuing digital certificates and providing digital certificate services, in order to establish the integrity and security of the digital certificate services it provides.

PART A – ANZ CERTIFICATE POLICY (SUBSCRIBER)

1. CERTIFICATES – PERMITTED USES

1.1 Purpose and Parameters of Digital Certificate Use

Your Digital Certificates are administered by ANZ and issued:

(a) to Users You nominate (and who have been approved by ANZ) to hold those Digital Certificates;

(b) solely for use by Users to:

(i) authenticate themselves to ANZ;

(ii) confidentially access Designated Products;

(iii) initiate instructions to an ANZ Group Member;

(iv) digitally sign messages; and

(v) communicate with ANZ,

and are not to be used for any other purpose.

ANZ expressly disclaims all unauthorised use, and any liability arising out of such unauthorised use and/or use of Digital Certificates for any purpose other than those set out in this Certificate Policy (Subscriber).

1.2 Designated Products

Authorisation to access or use any Designated Products must be independently obtained from ANZ for each relevant Designated Product.

1.3 Relying Party

The party relying on the Digital Certificate is ANZ or another ANZ Group Member.

2. VALIDITY PERIOD

The Validity Period of a Digital Certificate issued under this Certificate Policy (Subscriber) is 2 years.

3. AUDIENCE

This Certificate Policy (Subscriber) is only intended to be referred to by those persons who propose to subscribe or have subscribed to ANZ Digital Certificate Services.

PART B – ANZ CERTIFICATION PRACTICE STATEMENT

1. OVERVIEW

1.1 Application of this Certification Practice Statement

This CPS applies to the digital certificate infrastructure of ANZ known as ANZ Digital Certificate Services and relates only to infrastructure and Digital Certificates used by Subscribers to access Designated Products.

1.2 Digital Certificates

(a) A Digital Certificate is a data structure containing the Public Key of a cryptographic Key Pairs, each pair comprising:

(i) a Public Key which is publicly available; and

(ii) a Private Key that is known only to the User,

issued to a particular User. The Key Pair is generated in (and the Private Key can also be stored on) a physical device (eg. a card with an embedded chip).

(b) The Digital Certificate:

(i) identifies the issuer;

(ii) names or identifies a User;

(iii) contains the Public Key of the User;

(iv) identifies the Digital Certificate's Validity Period;

(v) is digitally signed by the issuer; and

(vi) is used in conjunction with the corresponding Private Key whenever the User creates a Digital Signature in order to authenticate the holder to ANZ.

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

1.3 What can You do with a Digital Certificate issued under ANZ Digital Certificate Services?

(a) Through use of the Key Pairs in a Digital Certificate You (as a Subscriber) can transmit data to ANZ by:

(i) appending Your Digital Signature to the message to authenticate that You sent the data (authentication) and to signify assent, consent, authorisation or agreement to its content (non-repudiation);

(ii) encrypting the data with ANZ's Public Key, (data confidentiality); and

(b) on receipt of the data, ANZ can then:

(i) apply Your Public Key to verify the integrity and authenticity of the data transmitted by You;

(ii) apply ANZ's own Private Key to decrypt the data that was sent by You and confirm that it has been transmitted confidentially; and

and in so doing, take comfort that You cannot dispute sending or creating the message (non-repudiation).

2. DOCUMENT IDENTIFICATION

Object Identifiers **(OID)** are globally unique identifiers, used to identify components within ANZ Digital Certificate Services. OIDs allow parties using ANZ Digital Certificate Services to identify and obtain from ANZ the actual certificate policies and certification practice statement applying to the use of the digital certificate services. The relevant OIDs for ANZ Digital Certificate Services are:

(a) Certification Practice Statement (i.e. this CPS)

1.2.36.5357522.5.2.1

(b) Certificate Policy (Subscriber)

1.2.36.5357522.5.2.3

3. ANZ'S RESPONSIBILITIES

ANZ operates ANZ Digital Certificate Services to provide an enhanced level of security for Transmissions You initiate to access Designated Products. It will receive applications for, process and issue Digital Certificates to You in accordance with this CPS and any other related documents. The ANZ Digital Certificate Services will be implemented in accordance with generally accepted security principles, covering computer hardware, software and procedures (including personnel practices) designed to ensure (to the extent reasonably possible) that:

(a) Your access to Designated Products is secure from intrusion and misuse;

(b) the systems used by ANZ (to allow such access) provide a high level of availability, reliability and correct operation and are suited to performing their intended functions; and

(c) instructions You give ANZ to Suspend or Revoke any compromised Digital Certificate are actioned promptly.

4. ANZ'S ROLES

In providing ANZ Digital Certificate Services, ANZ undertakes the following roles:

4.1 ANZ Root Certification Authority

The ANZ Root Certification Authority acts as the peak body for ANZ Digital Certificate Services. It issues Digital Certificates to a subordinate Certification Authority.

4.2 Certification Authority

The Certification Authority (including the system that automatically issues Digital Certificates on receipt of a valid request from a subordinate Registration Authority) ensures ANZ Digital Certificate Services are managed and operated within the policies and practices set out and referred to in this CPS and associated certificate policies. Under ANZ Digital Certificate Services, the Certification Authority:

(a) is subordinate to the ANZ Root Certification Authority;

(b) administers the Certification Authority operation, generating and issuing Digital Certificates through a subordinate Registration Authority to You and to Registration Authority Administrators;

(c) is responsible for ensuring that it and any subordinate Registration Authority operates in accordance with the Certificate Policy (Subscriber), this CPS and other internal policy documents governing the Certification Authority and Registration Authority operations; and

(d) attends to Digital Certificate Suspensions or Revocation requirements, as requested by a Registration Authority.

4.3 Registration Authority

The Registration Authority ensures all relevant requests comply with the CPS and associated certificate policies. Under ANZ Digital Certificate Services, all Registration Authorities:

(a) are subordinate to the Certification Authority;

(b) administer a Registration Authority operation confirming identity credentials of Subscribers and their Users, as part of the chain of trust issuing Digital Certificates to You and to Registration Authority Administrators;

(c) are responsible for monitoring that the Registration Authority, You and the Registration Authority Administrators operate in accordance with the relevant certificate policy, certification practice statement and other internal policy documents governing Registration Authority operation and Digital Certificate usage; and

(d) receive any Digital Certificate Suspension or Revocation requests from You, and forward these to the Certification Authority for actioning.

5. DIGITAL CERTIFICATE APPLICATION AND ISSUANCE

(a) Each application for a Digital Certificate is processed in accordance with the policies and practices outlined in Part B of this document.

(b) If all application criteria are met, including the satisfactory completion of identity checks, then ANZ may initiate the Digital Certificate issuance process as follows:

(i) a Digital Certificate issuance request is generated and digitally signed by a Registration Authority Administrator;

(ii) a Digital Certificate is then created by the Certificate Authority, if ANZ determines that it complies with Part B of this document; and

(iii) ANZ then securely delivers the Digital Certificate to the User or a person authorised by You to accept Digital Certificates.

(c) Any use of a Digital Certificate after receipt constitutes Your acceptance that the Digital Certificate is duly created and complete, and the Registration Information provided is true and correct.

6. DIGITAL CERTIFICATE REGISTRATION AND RENEWAL

6.1 Registration – Assignment of Distinguished Names

ANZ assigns a Distinguished Name to each User based on the Registration Information provided by the User or a person authorised by You to provide such information, in its absolute discretion, through the following process:

(a) Registration Authority Administrator (or other authorised individual) assigns a Distinguished Name;

(b) Registration Authority checks for:

(i) uniqueness within the ANZ Digital Certificate Services domain;

(ii) meaningfulness;

(iii) conformity to this CPS; and

(iv) grounds for rejection (eg. offensive or obscene),

before generation of a Digital Certificate; and

(c) Registration Authority Administrator processes the request and submits it to the Certification Authority.

6.2 Name claim dispute resolution procedure

If a dispute arises in relation to a Distinguished Name used by You (including one of Your Users), ANZ may in its absolute discretion and without liability to You (or the specific User), refuse to issue, Suspend or Revoke a Digital Certificate because of such dispute.

6.3 Routine Digital Certificate Renewal

Users are issued with new Keys and Digital Certificates prior to, or on expiry of, their current Digital Certificates without the requirement to re-check their identity and organisational status provided that:

(a) their current Digital Certificates have not been Revoked or Suspended;

(b) their Registration Information has not changed;

(c) the Registration Authority which checked their identity and organisational status continues to operate without compromise; and

(d) the most recent identity and organisational status check was performed not more than 5 years prior to the date of the current request for renewal.

If any of these conditions are not satisfied, Users applying for new Keys and Digital Certificates, on expiry of their current Digital Certificate, may be required to have their identity and organisational status verified in the same way as new Users.

Notwithstanding the above provisions, ANZ may at any time require a fresh identity and organisational status check for any User and/or Authorised Person where it, in its sole discretion, considers it necessary to maintain the security of the provision of ANZ Digital Certificate Services.

7. DIGITAL CERTIFICATE SUSPENSION OR REVOCATION

7.1 Circumstances for Suspension or Revocation

All Suspensions and Revocations will be handled promptly following ANZ's determination (in accordance with this section) that it is appropriate to Suspend or Revoke the relevant Digital Certificate. ANZ may Suspend or Revoke a Digital Certificate:

(a) on receipt by the Registration Authority of a request from a person authorised as per the "Suspension or Revocation request" section below (and ANZ will do so as soon as practicable after verifying that the request has been issued by a person with authority to issue it);

(b) if any of the following occurs:

(i) it is reasonably likely that the relevant Digital Certificate has been compromised;

(ii) there are reasonable grounds for believing that You have ceased trading;

(iii) if ANZ reasonably believes information needed to complete a Digital Certificate (including some or all of the Registration Information) has become inaccurate in a material respect;

(iv) any other change occurs that affects the accuracy and/or completeness of the Registration Information;

(v) a lawful direction is received from an authorised third party eg. a court order;

(vi) faulty or improper registration, Key generation or Digital Certificate issuance has occurred;

(vii) You tell ANZ that an User has ceased or will soon cease to be Your employee or agent;

(viii) You have not complied with any one of the obligations under the ANZ Electronic Banking Terms and Conditions or an event has occurred and is subsisting which entitles ANZ to terminate or suspend any product or service provided to You;

(ix) the ANZ Root Certification Authority Digital Certificate or the Certification Authority Digital Certificate in the chain of trust has been Suspended or Revoked; or

(x) any other circumstances arise which ANZ reasonably believes justifies Suspension or Revocation.

7.2 Suspension or Revocation request

ANZ will verify that a party who can make 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	Any relevant physical device and associated password and/or any other verification information that ANZ or its agents may request
Telephone	Telephone challenge and response answers and/or any other verification information that ANZ or any of its agents may request
Writing	ANZ's recorded signature for the person

The following persons or entities can request Suspension or Revocation:

PERSON/ENTITY	SUSPENSION/REVOCATION ACTION
User	Request ANZ to Revoke or Suspend their Digital Certificate at any time
Authorised Person	Request ANZ to Suspend or Revoke any or all of Your Digital Certificates
A person, nominated in the Registration Information, who certified or provided material evidence regarding the identity of You or any User	Request ANZ to Suspend or Revoke a Digital Certificate on the grounds that Registration Information has changed
Any other person/entity (including by court order or direction)	Request ANZ to Suspend or Revoke a Digital Certificate, providing ANZ is satisfied that the entity or person is lawfully: > empowered to do so; or > entitled to administer Your affairs, which relate to the Digital Certificate.
ANZ	Suspend or Revoke a Digital Certificate of: > its own employees, officers or agents; > You or any of Your Users; > any Certification Authority; or > the Registration Authority. in circumstances set out in this section

7.3 Notification of Suspension

If ANZ considers it, in its absolute discretion, to be prudent and practicable, it will advise You of the proposed Suspension or Revocation. ANZ may give You the opportunity to oppose the Suspension or Revocation unless the law provides otherwise.

If ANZ does not notify You prior to the Suspension or Revocation of a Digital Certificate it will take reasonable steps to notify the relevant User as soon as practicable that the Digital Certificate has been Suspended or Revoked.

If Suspension or Revocation of a Digital Certificate is proven to be unjustified, new Digital Certificates will be provided to You at ANZ's cost.

7.4 Cessation of Rights and Obligations

When a Digital Certificate is Suspended or Revoked:

(a) the validity of, and all rights associated with, the Digital Certificate cease immediately; and

(b) the obligations associated with the Digital Certificate will continue, to the extent that they are capable of being fulfilled.

8. SECURITY CONTROLS

8.1 Strong Authentication

ANZ maintains and enforces controls to ensure that the access to ANZ Digital Certificate Services for ANZ staff and designated authorised third parties is limited to enabling such personnel to conduct administrative and management tasks. Access to ANZ Digital Certificate Services is otherwise restricted to Authorised Persons and Users and then only to enable the conduct of authorised actions.

8.2 Digital Certificate Validity and Status Checks

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

check (including use of a Digital Certificate to authenticate or create a Digital Signature for a Transmission).

8.3 Security Audit Procedures

In order to maintain a secure environment within the ANZ Digital Certificate Services, ANZ will:

(a) record the following:

(i) administrative activity (which includes changes to policies and User directories) and other configuration changes;

(ii) access and signing activity, which covers all activity by Users including successful and failed logon attempts to ANZ systems; and

(b) back-up audit logs to a secure electronic back-up facility.

ANZ will provide You with copies of the security audit logs as they relate to Your usage of the ANZ Digital Certificate Services, upon written request.

8.4 Records Archival

During the operation of ANZ Digital Certificate Services, 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 physical and/or cryptographic protection.

8.5 Compromise and Disaster Recovery

ANZ maintains a disaster recovery and business continuity plan **(Business Continuity and Disaster Recovery Policy)** covering reasonably foreseeable types of disasters and compromises including:

(a) loss or corruption, including suspected corruption of computing resources, software or data; and

(b) compromise of the Certification Authority Key or any other Private Key relied on to establish the chain of trust in Digital Certificates issued under ANZ Digital Certificate Services.

8.6 Secure Data Centre

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 and complies with relevant ANZ internal policies (Physical Security Policy and Business Continuity and Disaster Recovery Policy).

8.7 ANZ Security Policies

ANZ maintains and complies with internal security policies in relation to logical access control, system and network configuration, information classification, information security management, cryptography, physical/personnel, technology acquisition and development, and compliance business continuity.

In particular, to ensure the adequate protection required for Certification Authorities, ANZ applies its internal:

(a) Information Security Management Policy (to ensure protection in the areas of confidentiality, integrity and availability); and

(b) Cryptography Policy (to ensure protection of Digital Certificates and cryptographic system data).

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

8.8 Personnel Controls

ANZ Group Members employ personnel and management practices and policies 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.

PART C – GLOSSARY

The following definitions apply throughout this document unless the context requires otherwise.

ANZ means the ANZ Group Member that is providing the ANZ Electronic Channel to You (and all of its branches and offices), including its successors, assigns and transferees.

ANZ Digital Certificate Services means the services provided by ANZ to issue Digital Certificates to Subscribers; and manage ANZ's internal systems and processes, so as to meet ANZ's responsibilities under this document, such that Subscribers can access Designated Products securely.

ANZ Electronic Channel means any electronic payments, receivables, information management or data delivery platforms and systems provided by ANZ allowing You to access and use any products and services.

ANZ Group Member means:

(a) Australia and New Zealand Banking Group Limited (ABN 11 005 357 522); and

(b) ANZ, part of ANZ National Bank Limited,

and any related company or entity in which either of them holds a direct or indirect ownership interest (including any subsidiary), including their respective successors, assigns and transferees and persons deriving title under any of them.

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

Authorised Person means any person appointed by You in such form as is acceptable to ANZ to perform certain functions on Your behalf including, to authorise applications, Suspensions and Revocations with respect to Digital Certificates issued on behalf of its Users.

Certification Authority has the meaning in Part B – ANZ's Roles – Certification Authority.

Designated Products means any ANZ Group Member product that is accessed via an ANZ Electronic Channel using Digital Certificates issued by ANZ.

Digital Certificate has the meaning in Part B – Overview – Digital Certificates.

Digital Signature means the transformation of an electronic record by one person using a Private Key and Public Key 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 User, generally a combination of name and organisation details.

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.

Private Key means the Private Key stored on a physical device and used to digitally sign messages.

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

Registration Authority has the meaning in Part B – ANZ's Roles – Registration Authority.

Registration Authority Administrator 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 You and Users must provide in order to apply for a Digital Certificate, including any personal information about an individual.

Relying Party means a party who may rely upon a Transmission.

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

Subscriber means a subscriber that uses (through nominated personnel) Digital Certificates issued under ANZ Digital Certificate Services to access any Designated Products. Your organisation is a Subscriber.

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

Transmission means an electronic message/data sent in digital form, which You authenticate with a Digital Signature.

User means an individual nominated by an organisation, or on its behalf, who is named or identified in a Digital Certificate issued in respect of the organisation.

Validity Period means the period within which a Digital Certificate can be validly used under ANZ Digital Certificate Services, being the period stipulated in each Digital Certificate and as varied by Suspension or Revocation performed in accordance with this CPS.

Australia and New Zealand Banking Group Limited ABN 11 005 357 522. ANZ Bank Limited. Item No. 77640 06.2011 W233568

anz.com