ANZ CERTIFICATION PRACTICE STATEMENT

CERTIFICATION PRACTICE STATEMENT

1. OVERVIEW

1.1 What is a Certification Practice Statement?

A certification practice statement 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.

This ANZ Certification Practice Statement (CPS) applies to one stream of 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.

All capitalised terms in this CPS are defined in Section 13(Glossary) and the provisions for interpretation and construction, severance, waiver and governing law contained in the ANZ Digital Certificate Terms and Conditions also apply to this CPS.

1.2 What is a Digital Certificate?

A Digital Certificate is a data structure with cryptographic Key Pairs, each pair comprising:

> a Public Key which is publicly available; and

> 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 Secure Token (eg. a card with an embedded chip). The Digital Certificate:

(a) identifies the issuer;

(b) names or identifies a Certificate Holder;

(c) contains the Public Key of the Certificate Holder;

(d) identifies the Digital 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 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?

Through use of the Key Pairs in a Digital Certificate:

(a) you (as a Subscriber) can transmit data to ANZ by:

(i) appending your Private Key to authenticate that you sent the data (authentication) and to signify assent, consent, authorisation or agreement to its content (non-repudiation); and

(ii) encrypting the data with ANZ's Public Key, (and in doing so, create a Digital Signature of the data); and

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

(i) apply your Public Key to authenticate that the data was sent by you (authentication);

(ii) apply ANZ's own Private Key to verify that the message has not been intercepted or tampered with by a third party during transmission (confirm integrity) and has been transmitted confidentially; and

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

An electronic message/data sent in digital form, which you authenticate with a Digital Signature, is referred to as a Transmission.

1.4 What other documents govern ANZ Public Key Infrastructure?

(a) This CPS, along with the Certificate Policy and the ANZ Digital Certificate Terms and Conditions comprise the Controlling Documents, governing your use of the ANZ Digital Certificate Services and the Digital Certificates issued through them.

(b) The Certificate Policy states the permitted uses and validity period for a Digital Certificate issued under it, along with the applicability of that certificate to a particular community and/or class of applications with common security requirements. Several certificate policies may be issued under the digital certificate services framework covering different usages. Those relating to ANZ Digital Certificate Services are further detailed in Section 2.

(c) The ANZ Digital Certificate Terms and Conditions set out the core legal (including liability) provisions governing:

(i) your application for issuance of Digital Certificates; and

(ii) your use of ANZ Digital Certificate Services and the Digital Certificates issued through them.

1.5 What role does ANZ play in the provision of ANZ Digital Certificate Services?

ANZ undertakes a number of roles which are more fully explained in section 3 of this CPS. ANZ acts as:

(a) ANZ Root Certification Authority – the peak body of ANZ Digital Certificate Services.

(b) Certificate Authority - generating and issuing Digital Certificates to Subscribers.

(c) Registration Authority - confirming identity credentials of Subscribers and their Certificate Holders.

ANZ must perform these roles in accordance with the Controlling Documents.

1.6 What services can you access with the Digital Certificates?

You can use your Digital Certificates to access Designated Products provided you have obtained the necessary authorisation relating to the relevant product.

1.7 What are your obligations in applying for and using ANZ Digital Certificate Services?

You must ensure that:

(a) you obtain independent legal advice about your rights and obligations under the Controlling Documents;

(b) prior to applying for a Digital Certificate, your Certificate Managers and each of your prospective Certificate Holders is appropriately trained in the use and security of Digital Certificates;

(c) your Certificate Holders keep secure all Private Keys, Secure Tokens and pass-phrases;

(d) Digital Certificates issued to you under ANZ Digital Certificate Services are only used for the limited purposes set out in the Certificate Policy;

(e) you notify ANZ immediately if you know or suspect that your Digital Certificates, Private Key or pass-phrases are no longer secure or protected from unauthorised use/access and in certain other circumstances (see ANZ Digital Certificate Terms and Conditions);

(f) you provide certain indemnities to the ANZ Group (see ANZ Digital Certificate Terms and Conditions); and

(g) you provide privacy consents regarding Personal Information you provide to ANZ.

1.8 What Liability does ANZ have and what are its Termination Rights?

(a) ANZ may in its absolute discretion terminate all services under ANZ Digital Certificate Services on 30 days notice to you (see ANZ Digital Certificate Terms and Conditions).

(b) Except as otherwise provided in the ANZ Digital Certificate Terms and Conditions, to the extent permitted by law:

(i) ANZ excludes all warranties and conditions; and

(ii) ANZ's liability under the Controlling Documents is limited

(see ANZ Digital Certificate Terms and Conditions).

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 that digital certificate services stream. 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 (Global Administrator) 1.2.36.5357522.5.2.2

(c) Certificate Policy 1.2.36.5357522.5.2.3

3. ANZ'S ROLES AND OBLIGATIONS

3.1 Responsibilities

ANZ operates ANZ Digital Certificate Services to provide an enhanced level of security for Transmissions you initiate to access Designated Products. In operating ANZ Digital Certificate Services, ANZ will comply with its obligations set out in the Controlling Documents. 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 Revoke any Compromised Digital Certificate are actioned promptly.

3.2 Roles

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

(a) ANZ Root Certification Authority

(b) Certification Authority

(c) Registration Authority

(d) ANZ Global Administrator

(e) Relying party

These are further discussed in the Sections below.

3.3 Role of 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.

3.4 Role of 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) is headed by a Certification Authority Officer

(c) administers the Certification Authority operation, issuing Digital Certificates through a subordinate Registration Authority to you and to ANZ Global Administrators

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

(e) attends to a Digital Certificate Suspension or Revocation requirements, as requested by a Registration Authority

(f) is governed by the following certificate policies:

(i) Certificate Policy (ANZ Global Administrator); and

(ii) Certificate Policy.

3.5 Role of Registration Authority

The Registration Authority (including the system that automatically processes Digital Certificate requests received from you or ANZ Global Administrator(s) ensures all relevant requests comply with the CPS and associated certificate policies. Under ANZ Digital Certificate Services, all Registration Authorities:

(a) are headed by a Registration Authority Officer

(b) are subordinate to the Certification Authority

(c) administer a Registration Authority operation, as part of the chain of trust issuing Digital Certificates to you and to ANZ Global Administrators

(d) are responsible for monitoring that the Registration Authority, you 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 Digital Certificate usage

(e) receive any Digital Certificate Suspension or Revocation requests from you, and forward these to the Certification Authority Officer or actioning

(f) are governed by the following certificate policies:

(i) Certificate Policy (ANZ Global Administrator); and

(ii) Certificate Policy.

3.6 Role of ANZ Global Administrators

ANZ Global Administrators:

(a) are responsible for administering individual system settings associated with Digital Certificates to comply with your requirements and those of Designated Products and the Digital Certificates themselves

(b) act as a contact point between ANZ Digital Certificate Services and you

(c) manage the chain of trust (established through the roles and hierarchy described in this Section) between ANZ and you, and are governed by the Certificate Policy (ANZ Global Administrator) and this CPS

(d) process your Digital Certificate applications; and

(e) Suspend and Revoke Digital Certificates.

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

3.7 Relying Party

ANZ and other members of the ANZ Group are the only relying parties under ANZ Digital Certificate Services. ANZ or the relevant members of the ANZ Group rely on you (including your Certificate Managers and Certificate Holders) to comply with all the terms of the Controlling Documents and the Designated Products Terms.

4. YOUR ROLE AND OBLIGATIONS

4.1 Your role

You use Digital Certificates issued under ANZ Digital Certificate Services to access Designated Products.

4.2 You must appoint a Certificate Manager

You must appoint and maintain at least one Certificate Manager. Each Certificate Manager appointed by you has the authority to appoint further Certificate Managers. Your Certificate Manager is able to initiate:

(a) requests for Digital Certificate issuance for your prospective Certificate Holders

(b) Suspension and Revocation requests with respect to any of your Digital Certificates

4.3 Your Other Obligations

You must ensure that your use of ANZ Digital Certificate Services and specifically your use of Digital Certificates to access relevant Designated Products is in accordance with the Controlling Documents. Your obligations (including specific obligations of your Certificate Managers and Certificate Holders) in relation to the use of ANZ Digital Certificate Services are set out in the Controlling Documents. You must also comply with the relevant Designated Products Terms, which will be provided when you procure the relevant Designated Product.

5. APPLICABILITY OF CERTIFICATES

Digital Certificates issued under ANZ Digital Certificate Services are used for identification and signing purposes only, enabling you to access Designated Products. These Digital Certificates must only be used for the limited purposes set out in the Certificate Policy and not for any other purpose.

6. PUBLICATION, REPOSITORY AND NOTIFICATION POLICIES

(a) The Certification Authority website can be accessed via www.anz.com/pki. This site includes a copy of current versions of relevant ANZ Digital Certificate Services documentation.

(b) Any amendments to the Controlling Documents will be notified to you, in accordance with the ANZ Digital Certificate Terms and Conditions.

(c) 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	Access to publications or notices

7. DIGITAL CERTIFICATE APPLICATION AND ISSUANCE

Each application for a Digital Certificate is processed in accordance with the policies and practices outlined in this CPS, including in particular, under sections 8 and 11.

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

(a) a Digital Certificate issuance request is generated within ANZ Digital Certificate Services systems

(b) a Digital Certificate is created, if ANZ determines that it complies with this CPS

(c) ANZ then securely delivers the Digital Certificate to you.

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.

8. DIGITAL CERTIFICATE REGISTRATION AND RENEWAL

8.1 Evidence of Identity

The business divisions responsible for relevant Designated Products (**Business Divisions**) have responsibility for ensuring that only authorised and known parties are able to access and use any Designated Products using Digital Certificates, and will determine and perform the requisite level of Evidence of Identity checking required for such activities. In some cases the responsibility for performance of these checks may be your responsibility, in which case you will perform the Evidence of Identity checks in accordance with any agreement with ANZ.

ANZ will protect any information collected by the Business Divisions for the purposes of Evidence of Identity in accordance with the laws of the Governing Jurisdiction.

8.2 Registration – Assignment of Distinguished Names

ANZ assigns a Distinguished Name to each Applicant based on the Registration Information, in its absolute discretion, through the following process:

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

(b) Registration Authority processes the request and passes it to the Certification Authority

(c) Certification Authority checks for:

(i) uniqueness within the ANZ Digital Certificate Services domain

(ii) meaningfulness

(iii) conformity to this CPS

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

before generating a Digital Certificate.

8.3 Name claim dispute resolution procedure

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

8.4 Routine Digital Certificate Renewal

Certificate Holders 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,

(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; and

(e) a request for renewal is made by your Certificate Holder or you at least 20 days prior to expiry of the Certificate Holder's current Digital Certificate

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

Notwithstanding the above provisions of this Section 8.4, ANZ may at any time require a fresh identity and organisational status check for any Certificate Holder and/or Certificate Manager where it, in its sole discretion, considers it necessary to maintain the security of the provision of ANZ Digital Certificate Services.

9. DIGITAL CERTIFICATE SUSPENSION OR REVOCATION

9.1 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 by section 9.2 (and ANZ will do so as soon as practicable after verifying that the request has been issued by a person with authority (under Section 9.2) 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 or an Insolvency Event has occurred

(iii) if ANZ reasonably believes Certificate 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 a Certificate Holder 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 Controlling Documents

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

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

9.2 Suspension or Revocation request

ANZ will verify that 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	Secure Token and associated pass-phrase and/or any other verification information that ANZ or its agents may request
Telephone	Telephone pass-phrase, challenge and response answers and/or any other verification information that ANZ or any of its agents may request

The following persons or entities can request Suspension or Revocation:

PERSON/ENTITY	SUSPENSION/REVOCATION ACTION
Certificate Holder	Request ANZ to Revoke or Suspend their Digital Certificate at any time
Certificate Manager	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 Certificate Holder	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 Certificate Holders; > any Certification Authority; or > the Registration Authority in circumstances set out in this Section.

9.3 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 Certificate Holder 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. ANZ's liability for unjustifiably Revoking a Digital Certificate is limited under the ANZ Digital Certificate Terms and Conditions.

9.4 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.

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

10. ANZ DIGITAL CERTIFICATE SERVICES TERMINATION

If ANZ decides to terminate the ANZ Digital Certificate Services, ANZ will give you a minimum of 30 days' written notice and will indicate the effective date of termination.

11. SECURITY CONTROLS

11.1 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 Certificate Managers and Certificate Holders and then only to enable the conduct of authorised actions.

11.2 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).

11.3 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, Certificate Holder directories, pass-phrase policies) and other configuration changes

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

(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.

11.4 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.

11.5 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

(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.

The Business Continuity and Disaster Recovery Policy used by ANZ meets the requirements of appropriate Australian and New Zealand Standards i.e. AS/NZS ISO/IEC 17799: 2001.

11.6 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).

11.7 ANZ Security Policy

ANZ maintains and complies with security policies on the following areas:

> logical access control
> system and network configuration
> information classification
> information security management
> cryptography

- physical/personnel
- technology acquisition and development
- compliance business continuity

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

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

11.8 Personnel Controls

ANZ Group employs 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.

12. CONTACT DETAILS WITHIN ANZ

Specific enquires regarding the usage of ANZ Digital Certificate Services are to be directed, in the first instance, to the Help Desk for the relevant Designated Product. Other enquiries or communications about this document may be addressed to:

Channel Manager
Transaction Banking & Specialised Lending
5/530 Collins Street
Melbourne VIC 3000
Australia.

13. GLOSSARY

ANZ means the ANZ Group Member that is providing the Digital Certificates 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:

(a) issue Digital Certificates to Subscribers and

(b) manage ANZ's internal systems and processes, so as to meet ANZ's responsibilities under Sections 3 and 7 to 11, such that Subscribers can access Designated Products securely.

ANZ Digital Certificate Terms and Conditions has the meaning in Section 1.4.

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

ANZ Group and **"ANZ Group Member"** means any related company or entity in which Australia and New Zealand Banking Group Limited (ABN 11 005 357 522) 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.

Applicant means an individual nominated by your organisation (through your Certificate Manager) as a person in favour of whom a Digital Certificate may be issued.

Certificate Manager means any person appointed in writing from time to time by your organization, to authorise applications, Suspensions and Revocations with respect to Digital Certificates issued on behalf of its Certificate Holders.

Certificate Holder means an individual nominated by your organization, or on its behalf, who is named or identified in a Digital Certificate issued in respect of your organization.

Certificate Information means information needed to complete a Digital Certificate and includes some or all of the Registration Information.

Certificate Policy (ANZ Global Administrator) means an internal ANZ certificate policy entitled same, as amended from time to time, applicable to ANZ Global Administrators.

Certificate Policy has the meaning in Section 1.4.

Certification Authority has the meaning in Section 3.4.

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

Certification Practice Statement and **CPS** has the meaning in Section 1.1.

Controlling Documents has the meaning in Section 1.4(a).

Designated Products means any ANZ Group product accessed via an electronic channel using an ANZ Digital Certificate issued by ANZ under the Controlling Documents.

Designated Products Terms means the terms and conditions relating to the access to and use of Designated Products.

Digital Certificate has the meaning in Section 1.2.

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, generally a combination of name and organisation details.

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

Insolvency Event means, in relation to a party, if:

(a) an order is made or a petition is presented or a resolution is passed for the administration, winding up or dissolution of that party;

(b) a receiver, administrator or other official or creditors' representative is appointed in respect of that party or any of the assets of that party;

(c) that party becomes insolvent for the purposes of any law;

(d) that party ceases or threatens to cease to carry on all or a substantial part of its business;

(e) the holder of any security takes possession of the whole or (in the opinion of ANZ) any material part of the property or assets of that party;

(f) that party enters into a compromise or arrangement with, or assignment for the benefit of, any of its members or creditors; or

something having a substantially similar effect to the above happens in connection with that party under the law of any jurisdiction.

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, as further described in Section 1.2.

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 Controlling Documents;

(b) any taxes or duties payable in connection with the Controlling Documents (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 means information about an individual.

Private Key means the Private Key used by a Certificate Holder to digitally sign messages on your behalf.

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 Section 3.5.

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 you and Applicants must provide in order to apply for a Digital Certificate, including any Personal Information.

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

Revocation/Revoke means to permanently terminate the Validity Period of a Digital 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) Digital Certificates issued under ANZ Digital Certificate Services to access any Designated Products. Your organization is a Subscriber.

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

Transmission has the meaning in section 1.3.

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.

You means your organization as Subscriber and where the context allows also specifically includes your Certificate Managers and Certificate Holders.

Australia and New Zealand Banking Group Limited (ANZ). ABN 11 005 357 522. Item No. ANZCPS0002 09/2010 W195552

anz.com