Certification Practice Statement

1. Introduction

1.1 Overview

This Certification Practice Statement (CPS) describes the practices and controls employed by the API Centre Digital Trust CA, operated by Payments NZ Limited and subordinate certificate authorities (CA) to issue, manage, revoke, and publish RFC5280 X.509 version 3 public key certificates for relying parties. It documents roles, responsibilities, technical and operational controls, and legal terms that govern the CA's issuance and lifecycle management of certificates.

This document is issued in accordance with RFC3647.

This CPS should be read in conjunction with the Certificate Policy (CP). In the event of any conflict between this CPS and the Certificate Policy, the CP will prevail.

Terms defined in the API Centre Terms and Conditions and used in this document have the meaning given to them in the API Centre Terms and Conditions.

1.2 Document Control

Version: 1.0
Publication Date: 2026-05-20

1.3 PKI Participants

1. **Certification Authority (CA):** API Centre Digital Trust CA, operated by Payments NZ Limited, including:
    1. Root CA,
    2. Intermediate Offline CA, and
    3. Intermediate Online CA (issuing CA).
2. **Registration Authority (RA):** Payments NZ Limited through its API Centre.
3. **Relying Parties:** API Standards Users
4. **Subscribers:** Persons (individuals or legal entities) acting for the Relying Party, devices or software systems that are under control of the Relying Party, which hold and use certificates issued under this CPS, including automation services used in the requesting of certificates.

1.4 Certificate Usage

Certificate usage is determined by individual certificate policies.

1.5 Policy Administration

Policy Administration is the responsibility of the API Centre[, subject to any amendment procedures set out in the [Register Standard]].

1.6 Definitions, Acronyms, and Interpretation

- Key terms used in this CPS are defined in:
  - Section 10 of this CPS;
  - The CPD Act;
  - The API Standards;
  - The Operational Standards; and
  - The API Centre Terms and Conditions

2. Publication and Repository Responsibilities

2.1 Publication of CA Information

1. The CA will publish certificates, certificate revocation lists (CRLs), certificate policies and this certification practice statement at https://ca.apicentre.co.nz.
2. Each Relying Party must create or upload certificates into the Register

2.2 Repository Management

1. The repository of information is managed by the API Centre and contracted suppliers.
2. Repository information includes Subscriber accounts and related information, certificates and CA information such as CRLs, CPs, CPS and certificate chain.
3. Content that is published in accordance with Section 2.1 of this CPS will be digitally signed and time-stamped to ensure authenticity and integrity.

2.3 Time or Frequency of Publication

1. CRLs will be published by the Intermediate Online CA at least every 24 hours or immediately during a high priority event.
2. Relying Parties must retrieve the CRLs at least once per hour.
3. Relying Parties must retrieve the CRLs programmatically, confirm signature validity and time-stamp match. Relying Parties must immediately commence use of CRLs once the checks have passed.

2.4 Access Controls for Repositories

1. Repository content that is published by the CA must be made publicly available and readable via HTTPS, using TLS v1.2 or higher.
2. Administrative repository functions are restricted to automation and may only be accessed as required by CA Operations staff. 'CA Operations' includes employees and contractors of Payments NZ Limited, including any third party service providers engaged by Payments NZ Limited to carry out its functions contemplated in this CPS.
3. The CA must ensure that staff access to the repository is controlled using multi-factor authentication and role-based access controls.
4. CA automation is via cloud platform management and will use strong authentication when required.

3. Identification and Authentication

3.1 Naming

1. Certificates use distinguished names (DN) in the subject field; name formats and constraints for each certificate profile are enumerated in Section 8.1. Duplicate subject names are not allowed.
2. Subject Alternative Names (SANs) using DNS entries are supported but must be registered with the API Centre prior to requesting a certificate.

3.2 Initial Identity Validation

1. For organisational Subscribers, identity proofing requires validated business registration documents and validated by the Subscriber's Nominated Representative (as defined in the Register Standard). Proof of New Zealand Business Number is required.
2. Names that are intended to be used with certificates require evidence (such as DNS registrar records).
3. Individuals that are acting on behalf of organisations will require multi-factor authentication, and will be added to the API Centre Register.
4. The validation steps differ by assurance level and are recorded in the RA log.

3.3 API Credential Establishment

1. Subscribers must retrieve a HMAC key from the API Centre Register in order to load their CA API credentials (public key) that will be used for subsequent API authentication.
2. Subscribers must keep their credentials current, renewing at least annually, and reasonably protect these from unauthorised access.
3. The use of the HMAC key is created and used in accordance with RFC8555, section 7.3.4,
4. The HMAC key is used to establish the public key credentials for authentication in CA API requests.

5. The CA API requests are authenticated according to RFC8555, section 6.2.
6. The CA will limit the HMAC key to a single use, which must occur within 5 days of issue.

3.4 Routine Rekeying Identity Validation

1. Rekey requests must use authenticated channels. If the rekey occurs within the certificate's validity period and Subscriber authentication is strong (e.g., existing private key or two-factor authenticated portal), revalidation is limited to confirming account control.
2. A Subscriber must notify the CA in the following circumstances as a full reproofing will be required:
    i. in the case of an organisational Subscriber, it:
        1. has a change of control (as 'control' is defined in the Companies Act 1993);
        2. changes its name;
    ii. in the case of an individual Subscriber, he or she:
        1. changes their name;
        2. moves to a residential address outside of New Zealand; or
    iii. where the Subscriber is subject to any other similar identity change to the above which could reasonably impact the accuracy of the Subscriber's name entries.

3.5 Revocation Request Validation

1. Revocation requests must be authenticated using one of the following:
    i. signed revocation request using the certificate's private key, submitted via CA API,
    ii. authenticated RA Register session, or
    iii. documented proof of authority from an authorised representative.
2. Emergency email, telephone or other communication channel revocations require corroborating identity evidence and follow-up written confirmation.

3.6 Certificate Renewal and Re-issuance

1. Renewals are treated as re-issuance when they involve new keys or changes to identity attributes.
2. Renewal requests submitted before expiration may use reduced validation steps if the Subscriber's identity and control were previously verified and no changes have occurred.
3. Renewal requests are submitted via the CA API.

4. Certificate Subscriber Life-Cycle Operational Requirements

4.1 Certificate Request

1. Subscribers may only request a certificate via submitting a CSR in the CA API, or another mechanism (e.g. manual issuance) as may be offered by the RA.
2. The Subscriber must be authenticated using the credential loaded in Section 3.
3. The Subscriber status in the Register must be active and appropriate for the requested environment.
4. All request fields (API and CSR) are validated against CA requirements and policy.
5. Names (Subject DN and any SANs) supplied are checked against those registered.

4.2 Certificate Issuance

1. Issuance is automated once CSR checks and Register checks have passed. The RA may optionally elect to issue certificates manually at its sole discretion.
2. The CA signs the certificate using an appropriate Intermediate Online CA private key.
3. The certificate attributes are set according to policy-compliant templates.
4. Issuance events are logged including timestamp, requesting Subscriber identity, certificate serial number and Register entity.
5. A copy of the public key is stored in the Register against the requesting Subscriber identity.
6. A maximum of ten (10) valid (not expired or revoked) certificates will be issued to and remain valid for a subscriber at any given time.

4.3 Certificate Acceptance

1. Subscribers must verify certificate attributes upon issuance.
2. Acceptance is recorded when the Subscriber API client completely receives the CA API response, or when the Subscriber deploys the certificate to the subject system.
3. Non-acceptance may trigger another issuance flow.

4.4 Key Pair and Certificate Usage

1. Subscribers are responsible for protecting private keys.
2. The definitions of allowed cryptographic algorithms, minimum key lengths, and permitted key usages are determined by each certificate profile.
3. Hardware-backed keystores (HSM, TPM, smartcard) are recommended for high-assurance.

4.5 Certificate Renewal

1. Renewal timeframe and validation scope are defined per certificate profile.
2. Renewal method is via request to the CA API in a manner consistent with Section 4.1.
3. Renewal via non-API methods is at the discretion of, and may be authorised by, the API Centre and may require additional validation steps as advised by the API Centre.

4.6 Certificate Revocation and Status Checking

1. Certificates must be revoked when:
    - a compromise is identified,
    - cessation of operation by Relying Party, or
    - a material misrepresentation in relation to the Relying Party identity is identified.
2. Revocation codes in RFC 5280 may be used to indicate revocation status.
3. Status is published in CRLs only, no OCSP responder will be made available.
4. Relying Parties and Subscribers will disallow any certificates listed in CRLs.

4.7 Certificate Suspension and Reactivation

1. Temporary suspension of a certificate is supported in any of the following cases: temporary loss of control, change in standards user subscription status, Subscriber request.
2. The suspension duration must not exceed 30 days. If the suspension exceeds 30 days, the certificate must be revoked.
3. Reactivation requires re-verification of the Subscriber's control and a documented RA approval.
4. Register status change may trigger a suspension.
5. Suspension may be requested by a Subscriber, or enacted by the RA.

5. Certificate Authority Life-Cycle Operational Requirements

The following provisions in this clause 5 describe the role and obligations of the CA:

5.1 Root and Intermediate CA creation

1. Offline keys are generated by a manual process, using CA platform FIPS 140-2 compliant HSM capabilities.
2. Offline root CA is self-signed, and valid for 20 years.
3. Intermediate Offline CA certificates are signed by the root CA, and are valid for 10 years.
4. Intermediate Online CA certificates are signed by the Intermediate Offline CA, and valid for 5 years.

5.2 Intermediate Issuance

1. Intermediate Offline CA certificates are signed by the root CA.
2. Intermediate Online CA certificates are signed by a corresponding Intermediate Offline CA.
3. Private keys for Intermediate Offline CA certificates are stored in HSMs and retrieved in a secure manner when used to sign CRLs or Intermediate Online CA certificates.

4. Private keys for Intermediate Online CA certificates are stored in protected keystores that are available to issue end-entity certificates programmatically.
5. Intermediate certificate issuance is a manual activity, using CA platform capabilities. It occurs after validation of all certificate signing request fields.
6. Issued certificates are installed after verification of issued certificate.
7. Issuance of intermediates will require notification to subscribers.
8. Updated certificates and chains are published in the RA repository.

5.3 Intermediate Renewal

1. Renewal of intermediate certificates can be either a rekey or renewal with existing keys.
2. Rekeying requires use of an HSM to generate a new key pair.
3. The renewal/rekey CSR must have all fields populated as per Section 5..
4. Renewal is a manual activity, using CA platform capabilities.
5. Renewal of intermediates will be notified to Subscribers.
6. If a renewal requires invalidation of a previous certificate the relevant CRL will be updated and published.
7. Issued certificates will be published by the API Centre in the RA repository.
8. Relying Parties and Subscribers must update certificate chains when new intermediate certificates are published.

5.4 Intermediate Revocation

1. An intermediate certificate must be revoked when:
    - a compromise is identified,
    - cessation of operation, or
    - if an issue with the certificate is identified.
2. Revocation codes in RFC 5280 may be recorded to indicate revocation reason.
3. On revocation, the CRL must be updated, signed and republished immediately by the API Centre.
4. Subscribers and Relying Parties must retrieve and apply the updated CRLs according to relevant CP.
5. After revocation of the certificate, stored keys may be destroyed if required.

5.5 CRL publishing

1. CRLs will be published in the RA repository at https://ca.apicentre.co.nz/crl.
2. CRLs must be retrieved by Subscribers and Relying Parties according to the relevant CP, but at least once every 24 hours.
3. On retrieval, the CRL is validated by the API Centre, including time-stamp and digital signature.

5.6 Root CA renewal

CA root renewal is a rare activity. As such, and because of the significant problems that can arise if performed incorrectly, each Relying Party must complete the following steps and perform validation at each step:

1. Determine whether rekeying or renewal is required.
2. If rekeying, generate a new key pair in offline HSM, securely storing the new private key.
3. If renewing with same key, retrieve the private key from offline HSM.
4. Generate new self-signed root CA certificate per Section 5.1.
5. Publish new root certificate in RA repository.
6. Re-sign any required certificate chains for Intermediate Offline CAs.
7. Record any audit logs for issuance process.

The RA will notify Subscribers and Relying Parties of new root CA.

Subscribers and Relying Parties must install the new CA certificate (and any updated certificate chains) in their trust stores.

5.7 End of CA Life Cycle and Key Destruction

In the event of CA termination or cessation, the CA will:

1. Publish a notice of termination.
2. Revoke affected subordinate certificates as required.
3. Securely retire and destroy private keys using NIST SP 800-88 or equivalent sanitisation procedures for cryptographic modules.
4. Retain archive records per legal requirements.

5.8 SDLC environments

Where a Relying Party wishes to operate in a SDLC environment:

1. An additional Root CA must be created for non-production usage.
2. An additional Intermediate Offline CA must be created for non-production usage, signed by the non-production Root CA.
3. An Intermediate Online CA certificate must be created for non-production usage.
4. The non-production Intermediate Online CA certificate must be signed by the non-production offline CA intermediate.
5. A CRL must be maintained for non-production CA issued certificates.
6. Revocation and rekeying for non-production certificates will follow the same processes as production CA.
7. A maximum of ten (10) valid (not expired or revoked) non-production certificates will be issued to and remain valid for a subscriber at any given time.

6. Facility, Management, and Operational Controls

6.1 Physical Security and Environmental Controls

The certificate authority is physically hosted on Google Cloud, and relies on Google Security.

1. Google Cloud is the infrastructure provider and implements physical and environmental security controls.
2. Google Cloud security documentation may be found here.

6.2 Procedural Controls

1. Standard operating procedures (SOPs) govern required activities, issuance workflows, emergency revocation, and incident response.
2. SOPs specify dual control, separation of duties, and mandatory witness requirements for critical operations.

6.3 Personnel Controls

1. Staff performing sensitive PKI roles must undergo background checks and role-based training.
2. Access to production systems is limited to authorised personnel with least-privilege practices and logged activity.

7. Technical Security Controls

7.1 Key Pair Generation and Installation

1. CA keys are generated in FIPS 140-2 Level 3 or higher HSMs.
2. Subscriber key generation is allowed on approved client devices or on HSMs based on profile requirements.
3. Key generation routines use approved cryptographic algorithms and entropy sources.

7.2 Private Key Protection and Cryptographic Module Engineering Controls

1. Private keys for CA Operations are stored in HSMs with tamper-evident controls.
2. Critical key material may use protections such as key wrapping, share-splitting, and multi-operator authorisation for usage.

7.3 Other Aspects of Key Pair Management

1. Google Cloud private CA cover key backup, restoration, and destruction.
2. Backups are encrypted and stored in controlled, auditable locations with access restrictions.

7.4 Activation Data

1. Activation of CA private keys requires multi-party authorisation via split activation keys and PINs.
2. Activation events are logged with operator identities, timestamps, and cryptographic proof where supported.

7.5 Platform Security Controls

1. Google manages security of the private CA service, key management and HSM layers.
2. Supplier manages the service provisioning and customisation to meet RA security requirements.
3. Platform automation is used to ensure securely configure and update environment.
4. All changes are logged and auditable.

7.6 Life Cycle Technical Controls

1. SDLC considerations are applied by the service supplier, including separate environments that allow for (at least) functional testing, quality assurance and security testing.
2. At least one environment will be maintained or available for support of the production CA.
3. Reports will be maintained in an auditable format that are accessible to the RA.

7.7 Network Security Controls

1. Physical network security is the responsibility of the cloud platform provider.
2. Logical network security and platform is provided by the API Centre.
3. Security testing is used to identify any issues with services provided over the internet.
4. Offline CA infrastructure is separated from online CA (intermediate issuer).

7.8 Timestamping

1. All critical events (issuance, revocation, key ceremony) are time-stamped using NTP servers synchronized to an authoritative source.
2. Where long-term validation is required, trusted timestamping authority services are used for archival records.

8. Certificate, CRL, and OCSP Profiles

8.1 Certificate Profile

1. Each certificate profile lists subject DN attributes, mandatory extensions, key algorithms, keyUsage, extendedKeyUsage, basicConstraints, and maximum validity periods.
2. Certificate policies are published at the RA Repository.

8.2 Certificate Revocation List (CRL) Profile

1. CRLs conform to X.509 v2 CRL format, containing:
    i. CRLNumber
    ii. AuthorityKeyIdentifier
    iii. nextUpdate
2. Delta CRLs are not currently utilised, as the volume of certificates issued is not considered to be substantial at this time.

8.3 Online Certificate Status Protocol (OCSP) Profile

1. No OCSP responder will be provided by the CA.

9. Compliance Audit and Other Assessments

9.1 Frequency and Scope of Audits

1. Independent third-party audits are conducted annually and after material changes to CA Operations.
2. Internal audits occur quarterly and cover controls, issuance logs, and compliance with this CPS.
3. User activity logs are monitored and may be audited on an ad hoc basis.

9.2 Identity and Qualifications of Audit Parties

1. Audits are performed by qualified, accredited firms with experience in PKI and information security audits.
2. Auditor independence is required; auditors may not have provided consultancy or implementation services to the CA in the prior 24 months.

9.3 Auditor's Relationship to Audited Party

1. Auditor engagements are governed by written contracts specifying scope, confidentiality, access rights, and reporting obligations.
2. Auditors report findings to the CA Management and relevant regulators.
3. Auditors' reports may be shared with Relying Parties at the discretion of the CA.

9.4 Topics Covered by Audit

Audits examine the following:

1. Issuance and renewal processes.
2. RA validation records.
3. Key management and HSM controls.
4. System change management.
5. Personnel access controls.

6. Repository integrity.

9.5 Actions Taken as a Result of Deficiency

At the discretion of the RA, the following applies:

1. Non-conformances prompt corrective action plans with timelines.
2. Material findings that affect certificate trustworthiness may require public disclosure, re-issuance, or revocation of affected certificates.

10. Definitions and Acronyms

10.1 Definitions

Any terms that are not defined elsewhere are defined here.

Term	Definition
RA Repository:	A web-accessible location where the RA (Registration Authority) will publish content, such as CA certificates, CP & CPS and CRL(s).
Offline HSM:	When using a cloud-based service it is not possible without significant effort (and some undesirable trade-offs) to use a truly offline HSM. Therefore, the term is defined as a privilege-separated HSM service, with restricted access, that does not participate or connect directly to the online issuing mechanism. The HSM is still certified to FIPS 140-2 requirements.

10.2 Acronyms

The document uses the following acronyms:

Acronym	Expansion
CA:	Certification Authority
CPD:	Customer and Product Data (Act)
CPS:	Certification Practice Statement
CRL:	Certificate Revocation List
CSR:	Certificate Signing Request
OCSP:	Online Certificate Status Protocol

Acronym	Expansion
HMAC:	Hash-based Message Authentication Code
HSM:	Hardware Security Module
SDLC:	Software Development Life-Cycle