# Certificate Policy

## 1. Introduction

### 1.1 Overview

This Certificate Policy (CP) describes rules and assurance levels for RFC 5280 X.509 public key version 3 certificates issued by the API Centre Digital Trust CA, operated by Payments NZ Limited and subordinate certificate authorities (CA). It defines applicability, responsibilities, and technical and procedural controls for certificate issuance and use.

This CP is prepared in accordance with RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and the Certification Practice Statement (CPS).

This CP should be read in conjunction with the CPS. In the event of any conflict between this CP and the CPS, this 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 name and identification

**Document title:** Payments NZ API Centre Certificate Policy

**Version:** 1.0

**Publication date:** 20 May 2026

### 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 Usage of certificates

1. **Permitted uses:** Certificates issued under this CP, in conjunction with their associated private key, may be used for the following purposes:
    a) MTLS server authentication and client authentication for Relying Parties.
    b) Digital Signatures on messages and tokens.
2. **Prohibited uses:** Relying Parties must not use certificates issued under this CP for:
    a) uses other than access to or use of open banking APIs;
    b) non-approved third party trust domains.
    c) general purpose web, API, database servers not associated with open banking.
    d) certificate issuance.

## 2. Publication and Repository Responsibilities

1. **Repository:** CA publishes certificates, CRLs, and this CP. at https://ca.apicentre.co.nz/cp (maintained by the CA).
2. **Publication frequency:** Certificates published upon issuance; CRLs published hourly or on revocation events; CP updated and re-published on changes.
3. **Access controls:** Repository data is publicly readable; administrative changes restricted to CA Operations staff and automation services. '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 CP.

## 3. Identification and Authentication

### 3.1 Naming

1. **Subject naming:** Subject Distinguished Name (DN) MUST follow the organisation's naming plan: CN, OU, O, L, ST, C. For definitions of these, please review RFC1779, section 2.3 and ITU-T x.520 SelectedAttributeTypes
2. **Name uniqueness:** Subscriber names MUST be unique within the issuing CA domain.

### 3.2 Initial identity validation

1. **Entity types:** Person/entity Subscriber, device, software service.
2. **Validation for humans:** The RA must verify government ID and corporate employment record or use corporate identity provider (IdP) authentication.
3. **Validation for devices/services:** The RA must verify proof of possession of private key (challenge), device serial, and owner registration via secure channel.

### 3.3 Authentication for renewal, rekey and revocation

1. **Certificate Renewal** A Subscriber may renew a certificate by authenticating to CA API using prior valid credentials and proof of key possession.
2. **Certificate Rekeying:** A Subscriber may rekey a certificate by authenticating to CA API using prior valid credentials and proof of key possession.
3. **Revocation requests:** A Subscriber may request the revocation of a certificate. The revocation request must be authenticated via the RA portal or CA API using multifactor authentication, or via authorised security operations with recorded approval.

## 4. Certificate Life-Cycle Operational Requirements

### 4.1 Certificate issuance

1. **Request:** A Certificate Signing Request (CSR) must be received via authenticated CA API; the CA API must confirm identity and issue the certificate using the Online Issuing Certificate.
2. **Key generation:** The recommended method of key generation is that the Subscriber generates a key-pair on a local device or HSM; alternatively, the CA may generate keys for constrained devices only with explicit policy exception granted by the RA at its discretion.

### 4.2 Certificate profiles

1. **Minimum key sizes:** Certificates must use RSA ≥ 4096 bits; ECDSA with curve secp384r1 or stronger.
2. **Validity periods:** End-entity TLS client/server certificates must have a validity period of at most 180 days; Message signing certificates must have a validity period of at most 365 days.
3. **Basic Constraints:** Subject type set CA = false; no path length constraint.
4. **Extensions:** KeyUsage (2.5.29.15.1) and ExtendedKeyUsage set per certificate type; certificatePolicy extension to include this CP Pointer.

#### 4.2.1 Network / MTLS certificate profile

1. **KeyUsage:** Certificates must have at least one key usage policy for signing: digitalSignature, keyEncipherment or keyAgreement only; extension is critical.
2. **ExtendedKeyUsage:** Set to clientAuthentication (1.3.6.1.5.5.7.3.2) and serverAuthentication (1.3.6.1.5.5.7.3.1) only.

#### 4.2.2 Message signing certificate profile

1. **KeyUsage:** Include digitalSignature, nonRepudiation, keyAgreement and keyEncipherment only; extension is critical.
2. **ExtendedKeyUsage:** No values set (not present).

### 4.3 Certificate renewal and rekey

1. **Renewal:** Certificate renewals are allowed provided the request is made within the last 30 days of validity after identity re-validation (if identity re-validation is required).
2. **Rekey:** Certificate rekeys require proof of key possession and any required re-validation steps.

### 4.4 Revocation

1. **Revocation reasons:** A Subscriber may request that the CA revoke a certification for the following reasons: Key compromise, cessation of its operation, change in key personnel (e.g. key personnel resign from the organisation), superseded, privilege withdrawn.
2. **Revocation request processing time:** Urgent revocations must be processed by the CA immediately; all other revocations must be processed by the CA within 24 hours of receiving the request.

3. **Status checking:** The CA must maintain a CRL; Relying Parties MUST check the CRL at least once per hour; no Online Certificate Status Protocol (OCSP) service is maintained.

## 5. Facility, Management and Operational Controls

### 5.1 Physical security

1. **Physical Premises:** No services will be hosted on servers on physical premises maintained by RA or CA; services must be cloud-hosted.
2. **Root CA:** Operated in an offline HSM environment within a physically secured data centre; multi-person access control for provider operations maintained by a cloud service provider.
3. **Issuing CA:** Hosted in hardened datacentres maintained by a cloud service provider; HSM backing for private keys.

### 5.2 Personnel controls

1. **Background checks:** All CA Operations staff must pass background checks and be subjected to confidentiality obligations regarding their work on the API Centre Digital Trust CA.
2. **Separation of duties:** CA admin, RA, and Audit responsibilities are separated.

### 5.3 Audit and logging

1. **Audit logs:** All CA Operations, cloud service attestations, key ceremonies, issuance, revocation, and administrative actions must be logged and retained by the CA for at least 7 years.
2. **Audit frequency:** The CA must complete an annual third-party audit of PKI operations and technical controls.

## 6. Technical Security Controls

### 6.1 Key generation and protection

1. **CA keys:** Generated in FIPS 140-2 Level 3 HSMs or software equivalent; private keys never leave HSM in plaintext.
2. **Subscriber keys:** Encouraged to be generated on-device or via software system automation; if generated by CA, key escrow is only allowed with contractually defined controls.

### 6.2 Cryptographic algorithm constraints

1. **Allowed algorithms:** RSA-PSS, ECDSA; symmetric algorithms for protocols per current best practices.
2. **Deprecation policy:** Algorithms and key sizes will be deprecated following industry guidance with at least 180 days' notice to Subscribers.

### 6.3 Time stamping and secure time

1. **Time source:** CA synchronises to NTP servers with authentication and monitors for anomalies.

### 7. Certificate, CRL and OCSP Profiles

1. **Certificate profile:** Conforms to X.509 v3 with required extensions: basicConstraints, keyUsage, subjectAltName as applicable, policyIdentifiers including this CP.
2. **CRL profile:** Follows X.509 CRL profile; delta CRLs supported for high-volume environments.
3. **OCSP:** No OCSP responder is maintained.

### 8. Compliance, Legal and Miscellaneous

#### 8.1 Compliance

1. **Audits:** CA Operations subject to annual compliance audit against this CP and related CPS.
2. **Breach notification:** CA will notify affected Relying Parties and Subscribers of material compromises according to contractual and legal obligations.

#### 8.2 Liability

1. **Limitations:** Payments NZ's liability under this CP and the CPS is limited in accordance with the API Centre Terms and Conditions.

#### 8.3 Fees

1. **No fees:** No additional fees will be charged to Subscribers for certificate issuance or renewal provided its Annual API Standards User Fee has been paid.
2. **Emergency actions:** The CA may charge a fee for emergency operations, if deemed appropriate, such as emergency revocation, rekeying and CRL publication.

### 9. OID and CPS Pointer

1. **No OID Registered:** No Object identifier is registered for this CP.
2. **CPS pointer:** The Certification Practice Statement that implements this CP is published at https://ca.apicentre.co.nz/cps and contains detailed operational procedures.

### Appendix A — Example Certificate Policy Identifier in a certificate

- certificatePolicies ::= { policyInformation { policyQualifiers = CPS pointer } }