Canadian Pacific Public Key Infrastructure Certificate Policy

This Certificate Policy is one of a family of documents describing the Canadian Pacific Public Key Infrastructure (PKI).The reader is strongly urged to also consult the Certification Practice Statement for the issuing Certification Authority.

TABLE OF CONTENTS

INTRODUCTION

Overview

A Public Key Infrastructure (PKI) system is a collection of Certificate Authorities (CAs), applications, people and procedures that issue digital certificates.

A Root CA at the top level, issues certificates to one or more Issuing CAs at the next level.

The Canadian Pacific Certificate Policy (CP) describes the manner in which certificates are requested, created, issued, renewed, managed, revoked and used by participants of the PKI.

This Canadian Pacific CP generally conforms to the Internet Engineering Task Force (IETF) "Public Key Infrastructure Extensions (PKIXs) Internet X.509 PKI Certificate Policy and Certification Practice Statement Framework" (also known as RFC 3647).

The Canadian Pacific PKI is used to provide digital certificates for:

1. Canadian Pacific employees
2. Canadian Pacific infrastructure systems such as servers and other devices
3. External parties with whom Canadian Pacific wishes to establish a digital trust relationship

Document Name and Identification

The Object Identifiers (OIDs) used for certificates issued under this CP are:

OID: 1.3.6.1.4.1.46125.100.100.1 – Canadian Pacific Public Key Infrastructure Certificate Policy.

PKI Participants

Certification Authorities

CA functions are performed by PKI administrators. CAs sign public certificates that bind Subscribers to their private keys within the PKI and are responsible for:

- Creating and signing digital certificates.
- Publishing certificate status through
  - CRLs
  - Online Certificate Status Protocol (OCSP).
- Requiring adherence to the Canadian Pacific CP.

- Creating, storing and recovering key pairs.

A CA may have other duties and a CA PKI administrator may have duties other than PKI administration. The PKI administrator may also perform duties on more than one CA.

A PKI administrator must be an employee of Canadian Pacific.

Registration Authorities

Registration Authorities' (RA) functions are performed by Canadian Pacific employees or contractors who have been approved by the CA.

RAs are responsible for:

- Establishing enrollment procedures and processing certificate requests
- Ensuring that certificate requests are transferred to/from the originator in a secure manner
- Verifying the identity and authentication of certificate applicants
- Managing revocation or certificate status change requests.
- Approving applications for issue, revocation or reissue of certificates

The RA may have other duties delegated by the CA or Canadian Pacific. The RA may also perform duties on more than one Certificate Authority (CA).

RA staff must be Canadian Pacific employees or contractors.

Subscribers

A Subscriber is a person, device or application that is issued a digital certificate. The certificate binds a public/private key pair to a single Subscriber. For a device or application, the person authorized by the organization may also be referred to as the Subscriber.

Subscribers must have a valid contractual business relationship with Canadian Pacific and agree to comply with the relevant PKI Operating policies and procedures.

End-Entity Subscribers are individuals or organizations that have obtained certificates for use related to Canadian Pacific products and services. End-Entity Subscriber certificates must only be used for authentication, confidentiality or message integrity.

End-Entity Subscribers include:

1. Humans
2. Hardware Devices
3. Software Applications

CA Subscribers sign other certificates or CRLs and may, in turn, administer any number of other CA Subscribers. CA Subscriber certificates may be used for authentication, confidentiality or message integrity.

Certificate Authority (CA) Subscribers may include:

1. Intermediate CAs who must only issue and sign certificates to Issuing Certificate Authorities CAs.

2. Issuing CA who must only issue and sign End-Entity certificates

Note that this policy does not impose any strict requirement for Intermediate CAs to exist except for operational convenience. There could be only a Root CA and Issuing CAs in existence at any point in time, with the function of the Intermediate CAs essentially being performed by the Root CA.

Relying Parties

RPs are persons or entities that trust a digital certificate issued by the Canadian Pacific PKI. RPs must have a valid business relationship and be contractually bound to comply with the relevant PKI Operating policies and procedures.

Other participants

None.

Certificate Usage

Appropriate Certificate Uses

Digital certificates may be used for

1. Integrity and authenticity of business transactions

2. Encryption of information

Prohibited Certificate Uses

Any usage not clearly specified in the Section headed “Appropriate Certificate Uses” on Page 13 above is prohibited.

Policy Administration

Organization administering the document

The Canadian Pacific Enterprise Security Team is responsible for administration of this document.

Contact person

The contact person for this document is the Director of Enterprise Security. Traditionally, this person reports to the Chief Information Officer.

Person determining CPS suitability for the policy

The Certification Practice Statement (CPS) is reviewed for suitability by the individual designated by the Director of Enterprise Security.

CPS approval procedures

The CPS must be approved by the following:

1. The Canadian Pacific Chief Information Officer
2. The Canadian Pacific Director of Enterprise Security

The CPS can contain information which could be used to launch attacks against the PKI. For this reason the CPS must not be made public and should only be disclosed once appropriate legal safeguards have been executed. An example of such a safeguard might be a non-disclosure agreement in the standard form used by Canadian Pacific and approved by the Canadian Pacific legal team.

Definitions and Acronyms

AES	Advanced Encryption Standard
CDP	Certificate Distribution Point
CP	Certificate Policy. **Note:** In this document he term "Canadian Pacific" is always written in full in order to avoid confusion.
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
Dual_EC_DRBG	Dual Elliptic Curve Deterministic Random Bit Generator. A pseudo-random bit generation algorithm known to be unsuitable for cryptographic use.
ECC	Elliptic Curve Cryptography

FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS, HTTP over SSL or HTTP Secure
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
NIST	(US Government) National Institute for Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (secret access code, usually numeric)
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comment
RP	Relying Party
RSA	Rivest, Shamir, Adleman key pair generation techniques
S/MIME	Secure Multipurpose Internet Mail Extension
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security

URL	Uniform Resource Locator
UTC	Coordinated Universal Time
X.509	ITU-T standard for certificates and their authentication framework

PUBLICATION AND REPOSITORY RESPONSIBILITIES

Repositories

All repositories must be implemented using standards-based methodologies such as LDAP, OCSP and HTTP(S).

A CA must have at least one certificate repository and one certificate status repository.

Certificates or CRLs may be published to a remote repository or OCSP responder. CRLs must be published to one or more Canadian Pacific websites such that they are accessible to both internal and external Subscribers.

CAs must publish certificate status information as well as this CP.

Publication of certification information

The Distribution Point (DP) field within each digital certificate identifies the publicly accessible location where the certificate status information is published.

A CA must publish certificate status information in the manner specified by the Canadian Pacific CPS.

Time or frequency of publication

Certificate information must be published immediately after issuance.

The Canadian Pacific CP is published whenever an amendment is required. The amended CP will normally be available 24 hours after being approved in the manner described under "Policy Administration" on page 13, above. This is done on a best-efforts basis.

The Canadian Pacific PKI must notify Subscribers and RPs of proposed changes to the CP and must publish the updated CP in the prescribed manner.

Other documents and agreements are published as required.

Access controls on repositories

Subscribers and RPs will be provided certificate status information by means of publicly-accessible CRLs or OCSP. There is no requirement to secure either CRLs or OCSP internally or externally, however Canadian Pacific may elect to implement controls intended to defend against attacks such as Denial of Service (DoS).

Certificate status information must be distributed in the manner outlined in the Canadian Pacific CPS and according to the section headed “Certificate Life-Cycle Operational Requirements” on page 20, below.

IDENTIFICATION AND AUTHENTICATION

Naming

Types of names

Each certificate must have a unique name for the Subscriber in the certificate Distinguished Name (DN) field. The DN must not be blank and must use printable characters.

Subscribers may request an alternative name in the Subject Alternative Name (SAN) extension field. The Canadian Pacific PKI may accept or reject the proposed SAN outright. Subscribers will be allowed at most three SAN proposals after which the SAN will be left blank.

Subscribers may be required to use other subject name fields or attributes including:

- Common Name (user or device name)
- User ID
- Email Address
- Organizational Unit
- Organization
- Locality
- State or Province
- Country

The Canadian Pacific CPS contains definitions for constructing Subscriber DNs and should be referred to for details.

Need for names to be meaningful

The English or French name by which a Subscriber is generally known to Canadian Pacific must be used. It is not permitted to use fictitious names.

Wildcard certificates may be signed with the following restrictions:

- The naming convention of *.<name>.CPR.CA is used (for example, *.PTC.CPR.CA).
- Wildcard certificates are normally used for applications that process transactions at multiple geographic locations (for example, active/active at multiple data centers) where "application stickiness" is required.
- No more than 30 servers shall use a single wildcard certificate.

Certificates containing a domain name not owned by Canadian Pacific ("foreign entity certificates") may be signed provided that:

1. Canadian Pacific has a business relationship with the foreign entity
2. Formal approval has been obtained from the foreign entity
3. An agreement is in place which explicitly permits such signing

Anonymity or pseudonymity of subscribers

Anonymous subscribers are not permitted.

Pseudonyms are not permitted.

Rules for interpreting various name forms

Names provided in languages other than English or French which require the use of non-Roman alphabets must be converted into a Romanized form satisfactory to the Subscriber and the CA. For example, Chinese names may be converted into Pinyin.

Uniqueness of names

Names must be unique within the context of the Canadian Pacific PKI.

Recognition, authentication, and role of trademarks

Certificate fields may not contain trademarks or other proprietary information unless prior approval has been obtained from the holder. An appropriate notation must be used to identify such information where it exists.

Initial Identity Validation

Method to prove possession of private key

Certificate signing (enrollment) requests must be submitted in the form of a self-signed certificate to demonstrate possession of a private key.

Authentication of organization identity

A Subscriber must be authorized to initiate an enrollment request on behalf of the organization for which it is being requested. The enrollment process must securely establish enough details about the Subscriber to permit the RAs to validate the request.

The RAs must verify the identity of the Subscriber and the Canadian Pacific business relationship.

The details used to verify the Subscriber's identification must be kept for at least six months.

Authentication of individual identity

Authorized individuals may submit requests to become End-Entity Subscribers to a CA.

The Subscriber must:

1. Generate a request that meets Canadian Pacific PKI requirements
2. Deliver an authenticated request to the RA in a secure manner (e.g. S/MIME)

The RA has the responsibility, on behalf of a CA, to:

1. Verify that all of the prerequisites have been successfully completed
2. Authenticate the entity according to the type of certificate being requested
3. Verify that the certificate request has made in a secure manner
4. Process the certificate request as defined by the Canadian Pacific CPS

The RA must keep a record of the certificate processing documentation for at least six months.

Non-verified subscriber information

Not applicable

Validation of authority

The RA will verify that certificate requests are only made by properly authorized entities.

Internal entities will be verified against company databases such as those used to administer user login IDs or for Human Resource (HR) purposes. Computer systems and applications will be verified against internal DNS records, by visual inspection or by consulting project documentation.

In the case of entities external to Canadian Pacific the RA must verify that a contract or other form of written authorization exists prior to processing the certificate request.

Criteria for interoperation

Cross-certification within CAs or with external CAs (for example, other railroads) is supported.

Identification and Authentication for Re-key Requests

Identification and authentication for routine re-key

The requirements are the same as for the initial certificate signing request.

RAs must keep a record of the type and details of the re-keying request including the identity and authentication of the person making the request for at least six months.

Identification and authentication for re-key after revocation

The requirements are the same as for the initial certificate signing request.

RAs must keep a record of the type and details of the re-keying request including the identity and authentication of the person making the request for at least six months.

Identification and Authentication for Revocation Requests

RAs must authenticate a request for revocation of a certificate in the same manner as the initial certificate signing request.

RAs must keep a record of the type and details of the revocation request including the identity and authentication of the person making the request for at least six months.

CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Certificate Application

The act of applying for a certificate does not oblige a CA to issue a certificate. A CA may reject the request outright or return it to the requestor indicating that additional information is required.

Subscriber information must be complete, validated and accurate with full disclosure of required information in connection with a certificate request.

Subscribers requesting a certificate may be required to consent to a Subscribers Agreement or equivalent document in the form prescribed by Canadian Pacific’s Legal Department. The requirement can be imposed either at the time of registration or upon certificate acceptance.

Who can submit a certificate application

Employees and contractors of Canadian Pacific may submit certificate applications.

External entities having a valid business relationship with Canadian Pacific may submit applications for certificates.

Enrollment process and responsibilities

In the most general case, the enrollment process will normally be initiated by the Subscriber generating a key pair from which they generate a self-signed Certificate Signing Request (CSR) and securely submitting it to the RA.

There also exist other means (via Active Directory for example) for Subscribers to request certificates in an automated fashion. The Identification and Authorization activities are then performed via the system being used, as are the key pair generation and Certificate Signing Request.

Certificate Application Processing

Performing identification and authentication functions

However the Certificate Signing Request is generated, the RA will verify the identity of the Subscriber and ensure that the request has been submitted in a secure manner acceptable to the RA. The RA will also verify the provided Subscriber data for completeness and accuracy.

The RA may require the Subscriber to furnish additional information and it is the responsibility of the Subscriber to supply accurate and complete information when requested to do so.

Approval or rejection of certificate applications

Upon receiving and processing a certificate request, the RA may take any or all of the following actions at their sole discretion:

1. Reject the request outright with no explanation

2. Reject the request and provide an explanation which the RA deems to be sufficiently complete and accurate

3. Reject the request with advice as to what course of action could be followed in a subsequent application

4. Continue to process the request but demand additional information from the Subscriber

5. Process the request by handing it over to the CA for certificate issuance.

Time to process certificate applications

The RA will act on and process a certificate application on a best-efforts basis.

Certificate Issuance

CA actions during certificate issuance

The CA will validate that the request for certificate issuance has come from a valid RA.

The CA will examine the certificate request and verify that all required information has been provided.

The CA will verify that the system time on the Issuing CA machine is correct before initiating a certificate signing procedure.

The CA will verify that there is no evidence of tampering with either the Hardware Security Module (HSM) or Issuing CA machine.

Notification to subscriber by the CA of issuance of certificate

If the request has been verified to be valid, the CA will issue the requested certificate.

Certificate Acceptance

Conduct constituting certificate acceptance

Use of a certificate for any purpose constitutes acceptance.

By using and therefore accepting the certificate the Subscriber agrees to comply with the terms of any policies referenced within the Certificate Policies (CPs) field of the certificate.

Publication of the certificate by the CA

A CA is responsible for repository and publication functions. A CA must publish certificates in a repository based on the certificate publishing practices defined in the Canadian Pacific CPS.

Certificates may either be sent by e-mail to the Subscriber or published to corporate repositories such as Active Directory or LDAP. This allows other subscribers to conveniently locate and use the subject's certificate.

Of course, the private key is never published to any repository.

Notification of certificate issuance by the CA to other entities

Publication of certificates in Corporate repositories is considered notification to RPs for Canadian Pacific Internal Subscribers.

E-mail will generally be used to notify all other Subscribers and RPs that a certificate has been issued.

Key Pair and Certificate Usage

Subscriber private key and certificate usage

A CA must only use its private key to sign certificates and CRLs for production use. A CA must not transfer its private key from the platform on which it was generated (normally an HSM) to another platform except for business recovery or load balancing purposes. In any case the private key must never be transported or stored externally to the HSM in an unencrypted form.

A CA must use commercially reasonable efforts to ensure that issued certificates and associated key pairs are used only for functions related to the legitimate business of Canadian Pacific.

Private keys used by a RA for authentication in order to operate the RA applications, must not be used for any other purpose.

The Subscriber must only use certificates issued under this policy for access to Canadian Pacific production systems. The certificates must not be used in a test environment.

A separate process is available for requesting test certificates and they are issued under a separate Certificate Policy.

Relying party public key and certificate usage

An RP should always verify that a Subscriber's certificate is appropriate for the intended application prior to use.

A publisher certificate is a certificate with code or document signing extensions. The Canadian Pacific CA may sign publisher certificates with document signing extensions for internal and external use provided that the intended purpose is to securely exchange documents for the purpose of conducting Canadian Pacific’s business.

The Canadian Pacific CA may sign publisher certificates with code signing extensions for internal production use only.

An email encryption certificate is a certificate with email encryption extensions. An email signing certificate is a certificate with email signing extensions. The Canadian Pacific CA may sign email encryption and signing certificates for internal and external use provided that the intended purpose is to exchange e-mail securely for the purpose of conducting Canadian Pacific’s business.

Certificate Renewal

Circumstance for certificate renewal

Certificates may be renewed provided that

1. The certificate life has not expired.

2. Subscriber name and attributes are unchanged

3. The associated private key remains uncompromised

4. Re-verification of the Subscriber's identity is not required

Given that all the above conditions hold true, a renewal request may be submitted to the RA.

If any of the above conditions are not satisfied, the certificate must be revoked and a new certificate issued.

It may also be deemed necessary to renew a certificate if a CA certificate is re-keyed.

Who may request renewal

The Canadian Pacific Issuing CAs and any Subscribers may request renewal of their certificates.

The Canadian Pacific Issuing CAs may renew a certificate without a corresponding request if the signing certificate is re-keyed.

Processing certificate renewal requests

In the case of the Issuing CAs, the certificates will be renewed by the Root CA. The CA will ensure that the details contained within the Issuing CA certificate are still valid.

In the case of End User certificates, the RA will verify that the Subscriber details in the certificate are still valid.

Notification of new certificate issuance to subscriber

Notification will be as described in the Section headed "Notification to subscriber by the CA of issuance of certificate" on page 22, above.

Conduct constituting acceptance of a renewal certificate

Acceptance will be as described in the Section headed "Conduct constituting certificate acceptance" on page 22, above.

Publication of the renewal certificate by the CA

The certificate will be published as outlined in the section headed "Publication of the certificate by the CA" on page 22, above.

Notification of certificate issuance by the CA to other entities

Notification of other entities will be done in the manner described under "Notification of certificate issuance by the CA to other entities" on page 22, above.

Certificate Re-key

Circumstance for certificate re-key

Re-keying a certificate consists of creating a new certificate with a new public key and serial number while keeping the subject information the same. The new certificate may have a different validity date, key identifiers, CRL and OCSP distribution points, and signing key.

The CA will revoke the old certificate and may not further re-key, renew, or modify the old certificate.

Who may request certification of a new public key

The CA may initiate a certificate re-key at the request of the certificate subject or at the CA's own discretion.

Processing certificate re-keying requests

If the Private Key and any identity and domain information in a certificate have not changed, then the CA may issue a replacement certificate using the previously provided CSR. Otherwise, the Subscriber must submit a new CSR. The RA will re-use existing verification information unless re-verification is required because the RA believes that the information has become inaccurate.

Notification of new certificate issuance to subscriber

Notification will be as described in the Section headed "Notification to subscriber by the CA of issuance of certificate" on page 26, above.

Conduct constituting acceptance of a re-keyed certificate

Acceptance will be as described in the Section headed "Conduct constituting certificate acceptance" on page 26, above.

Publication of the re-keyed certificate by the CA

The certificate will be published as outlined in the section headed "Publication of the certificate by the CA" on page 26, above.

Notification of certificate issuance by the CA to other entities

Notification of other entities will be done in the manner described under "Notification of certificate issuance by the CA to other entities" on page 27, above.

Certificate Modification

Circumstance for certificate modification

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate in non-essential parts of names or attributes provided that the modification otherwise complies with this CP.

The new certificate must have the same subject public key.

After modifying a certificate, The RA must revoke the old certificate and will not further re-key, renew, or modify the old certificate.

Who may request certificate modification

Subscribers or the RA may request certificate modification.

Processing certificate modification requests

After receiving a request for modification, the RA verifies any information that will change in the modified certificate. The RA and CA will only issue the modified certificate after completing the verification process on all modified information.

The CA will not issue a modified certificate that contravenes any part of this CP.

Notification of new certificate issuance to subscriber

Notification will be as described in the Section headed "Notification to subscriber by the CA of issuance of certificate" on page 26, above.

Conduct constituting acceptance of modified certificate

Acceptance will be as described in the Section headed "Conduct constituting certificate acceptance" on page 26, above.

Publication of the modified certificate by the CA

The certificate will be published as outlined in the section headed "Publication of the certificate by the CA" on page 26, above.

Notification of certificate issuance by the CA to other entities

Notification of other entities will be done in the manner described under "Notification of certificate issuance by the CA to other entities" on page 27, above.

Certificate Revocation and Suspension

Circumstances for revocation

A certificate must be revoked or otherwise invalidated:

1. When a Subscriber fails to comply with obligations set out in this CP or in the CPS
2. When it is discovered that the certificate was issued erroneously or fraudulently
3. When the basis for any information in the certificate changes
4. When there is a change in the business relationship under which the certificate was issued
5. When a Subscriber is no longer using a certificate for the purpose for which it was issued
6. Upon suspected or known compromise of the private key or of the media holding the key
7. Upon notification of termination of an employee or Subscriber
8. When the certificate has been issued to an ineligible Subscriber
9. When a Subscriber no longer needs access to Canadian Pacific systems or services
10. When technical considerations dictate that the certificate is no longer suitable for its intended use.
11. When the certificate was used to sign, publish, or distribute malware or other harmful content.

Who can request revocation

The Canadian Pacific CAs and RAs may revoke a certificate without receiving a request and without reason.

More generally, any authorized party may request revocation of a certificate for problems related to fraud, misuse, or compromise. Authorization to request revocation will be verified by the RA and CA. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

A legally recognized representative of either party to a cross-signed CA certificate may request revocation.

A certificate will be revoked if there is sufficient evidence of compromise or loss of the private key.

Procedure for revocation request

A CA must make certificate revocation data available to Subscribers and RPs. The Issuing CA must notify a Subscriber when a certificate bearing a Subscriber’s identity is revoked. The notice of revocation must be posted to a CRL as soon as possible. The address of the CRL must be defined in the certificate.

All requests for revocation must be submitted to the CA or RA authenticated in the same manner as the initial certificate request.

The authenticated revocation request and any resulting actions taken by the Certificate Authority (CA) must be recorded and retained for a minimum of one (1) year. When a certificate is revoked, justification for the revocation must be documented.

Revocation request grace period

All PKI Subscribers and RPs are required to request revocation as soon as possible if the Private Key is lost or compromised or if the data in the certificate is no longer valid.

Canadian Pacific will report to its Subscribers and RPs the suspected compromise of any of its CA private keys within one hour of discovery.

Time within which CA must process the revocation request

For compromise of Root CA or Issuing CA private keys the revocation must be issued within one hour.

For Subscriber certificates, revocation must occur within 24 hours.

Revocation checking requirement for relying parties

RPs should check the status of certificates against current CRLs prior to use. If the RP stores a copy of the CRL, they must retrieve a 'fresh' CRL at least daily. CRL checks must also include authenticity and integrity verification.

CRL issuance frequency (if applicable)

CRLs are issued automatically as soon as possible whenever one or more certificates are revoked and at least daily if there has been any change.

Maximum latency for CRLs (if applicable)

CRLs for End Entity subscribers are posted automatically to the online repository within a commercially reasonable time, usually minutes after generation.

On-line revocation/status checking availability

The CRL and OCSP responder services will be managed to the same availability target as other Canadian Pacific internal systems.

On-line revocation checking requirements

Refer to "Revocation checking requirement for relying parties" on page 28, above.

Other forms of revocation advertisements available

None

Special requirements re key compromise

Canadian Pacific uses commercially reasonable efforts to notify Subscribers and RPs if it discovers or suspects the compromise of a Private Key.

Circumstances for suspension

A certificate may be suspended or revoked whenever any of the conditions listed in "Circumstances for revocation" on page 26, above are suspected or known. A CA may, at its discretion, suspend a certificate rather than revoking it pending validation of the revocation request. During the suspension period, the suspended certificate must be listed on a CRL. Suspensions remain in effect until the CA determines whether the certificate will be revoked or reinstated.

Who can request suspension

Same as "Who can request revocation" on page 27, above.

Procedure for suspension request

Same as "Procedure for revocation request" on page 27, above.

Limits on suspension period

When a certificate is suspended pending verification of a revocation request, the suspension period must be long enough to validate the revocation request.

At the end of the suspension period, the CA will reinstate, revoke or extend the suspension period of the certificate.

Certificate Status Services

Operational characteristics

Canadian Pacific makes certificate status information available via both CRLs and OCSP.

The OCSP responder service is the preferred method of checking for certificate revocation as it is expected to provide more current and timely information than the CRLs.

CRL and OCSP responses are provided in a commercially reasonable time which is typically within a few seconds after the request is received, subject to intervening network latency.

Service availability

CRL and OCSP responders are managed to meet or exceed the same availability targets as other Canadian Pacific internal systems.

Optional features

None.

End of Subscription

A Subscriber’s service ends if its certificate expires without renewal or is revoked.

Key Escrow and Recovery

Key escrow and recovery policy and practices

CA private key(s) must not be escrowed.

Canadian Pacific may escrow Internal Subscriber private keys used for e-mail and data encryption on Canadian Pacific equipment. Normally this will only be done in order to facilitate recovery of encrypted data belonging to Canadian Pacific and created during the Subscriber’s employment with Canadian Pacific.

Retrieval of private keys from escrow is considered to be a very unusual event and only to be exercised in extreme circumstances such as employee termination or in support of criminal investigations where supported by the necessary search warrants.

In order for Subscriber private keys to be retrieved from escrow, authorization is required from the Canadian Pacific Chief Information Officer as well as the Director of Enterprise Security.

Session key encapsulation and recovery policy and practices

Not specified.

FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

Physical Controls

The CA facilities must provide the physical security controls as outlined in the Canadian Pacific CPS.

The Root CA must be stored in secure facilities managed by CP Police who will also ensure that chain of custody is maintained for all Root CA components.

Issuing CAs are maintained in commercial-grade data centres together with other Canadian Pacific production systems.

Site location and construction

The access control systems must be inspected at least bi-annually by qualified personnel from the Enterprise Security Team.

Access control and monitoring systems must have an Uninterruptable Power Supply (UPS) system. The UPS system must be inspected at least annually

Documentation must be retained for at least six months.

Physical access

The physical access controls are defined in the Canadian Pacific CPS.

Power and air conditioning

CA facility management must ensure that

- Power
- Air conditioning
- Water exposures
- Fire suppression
- Fire prevention and protection
- Other environmental controls

can support the operation of the CA systems.

Media storage

Backups of key material must be secured to prevent inadvertent or intentional disclosure.

Waste disposal

The CA is responsible to ensure that any material of a sensitive nature is securely disposed of. That includes, but is not limited to:

- anything that might contain full or partial private keys
- hardware components from any CA systems
- hand written notes
- expired system backups

Off-site backup

The Root CA must be securely backed up at least annually.

Issuing CAs must be securely backed up at least weekly.

Secure backups for the Root and Issuing CAs must be stored offsite for disaster recovery purposes.

Procedural Controls

Trusted roles

At a minimum, critical CA functions must be performed with knowledge and control of more than one person:

- Generation of a new CA key pair
- Replacement or renewal of a CA key pair
- Change in the certificate profile security policy

PKI administrators must be subject to a combination of controls:

- Restricted access to the facility
- Operating system audit logs, including logon on logoff
- Audit logs of certificate creation, issuance, suspension, revocation and modification

Number of persons required per task

Subject to the constraints outlined above:

- Critical CA functions require a minimum of two people present at all times.
- Routine PKI administration tasks may be done by a single individual

The CA shall ensure that no single individual may gain access to Subscriber private keys stored by the CA.

Identification and authentication for each role

All CA personnel must have their identity and authorization verified before they are:

- Allowed physical access to a CA facility
- Allowed logical access to a CA system
- Issued a certificate to perform the CA operator's role

All certificates issued to CA personnel:

- must be attributable to a single individual
- must not be shared
- must be restricted to actions authorized for that role

Roles requiring separation of duties

Roles requiring a separation of duties include:

1. Critical PKI functions
2. PKI administrators responsible for day to day tasks
3. Routine system maintenance, backups and similar functions
4. Collection and analysis of system audit logs
5. Auditing systems and procedures
6. Physical security of the locations where CA systems are operated

Personnel Controls

Qualifications, experience, and clearance requirements

In addition to the normal Canadian Pacific employee requirements, CA personnel must also have training, qualifications, and experience in the operation of PKI systems.

Background check procedures

Standard Canadian Pacific background checks must be performed on all CA operations personnel.

Training requirements

Employees must maintain skill levels that are consistent with accepted industry practices in order to continue acting in trusted roles.

Retraining frequency and requirements

Not specified

Job rotation frequency and sequence

Not specified

Sanctions for unauthorized actions

In the event of actual or suspected malfeasance by a person performing PKI-related duties the CA must immediately revoke all access to the CA system by that person.

A CA may revoke a certificate when an entity fails to comply with obligations set out in this CP and the Canadian Pacific CPS.

A CA may suspend a certificate at any time if a CA knows or suspects conditions that may lead to a compromise of keys or certificates.

Independent contractor requirements

The CA shall ensure that contract personnel satisfy the same personnel security requirements with respect to appointment, training and background checks as those applicable to CA employees.

The CA must limit contractor physical access to the CA facility and contractor personnel must be escorted while in the CA facilities.

Documentation supplied to personnel

PKI administration personnel must be provided with copies of this CP and the Canadian Pacific CPS.

Audit Logging Procedures

Types of events recorded

A CA must record in audit logs successes and failures of all events relating to the security of that CA system. Logs must include the date and time of the event what person or entity caused the event.

The Canadian Pacific CPS must contain details regarding what information is logged.

It is not permitted for an individual causing an event to sign off on the event.

Frequency of processing log

At a minimum, a review must be conducted once every 90 days for online CAs and annually for offline CAs. Actions taken following these reviews must be documented.

Retention period for audit log

A CA must retain audit logs pertaining certificate management for at least six months after the certificate is revoked or expired.

Other audit record retention must conform to standard Canadian Pacific retention practices.

Protection of audit log

Electronic audit logs must be protected from unauthorized viewing, modification or deletion.

Manual logs must be physically protected from unauthorized viewing, modification or deletion.

Audit log backup procedures

Audit logs must be backed up or copied as per normal Canadian Pacific practices.

For offline CAs audit logs must be backed up immediately following each ceremony generation.

Records pertaining to management of a certificate must be retained for at least six months after the certificate is revoked or expired.

Audit collection system (internal vs. external)

Automatic audit logs must start recording at system startup and only end at system shutdown.

Notification to event-causing subject

No notice is required to be given to the individual or entity that caused an event.

Vulnerability assessments

Vulnerability assessments must be conducted following Canadian Pacific's normal business processes.

For computers and systems the frequency and type of assessment is dictated by the Enterprise Security Team.

Physical access to facilities holding offline root CAs will be assessed for vulnerability by Canadian Pacific Police.

Records Archival

Types of records archived

The following types of records are archived:

1. Root CA key generation script, video and hand-written certifications by participants. Key signing procedure when Root CA signs Issuing CA keys. Root CA system logs related to system operation and function of the CA software. HSM audit logs.

2. Issuing CA system logs related to system access and operation of the CA software. Records of certificates requested and issued. HSM audit logs.

3. Manual sign-in and sign-out sheets maintained at secure facilities where Root CAs are stored.

Retention period for archive

Root CA archives are retained for twice the life of the Root Private Key.

Issuing CA archives are retained for three years.

Manual sign-in and sign-out sheets are maintained according to Canadian Pacific Police standard policies.

Protection of archive

Archives must be protected from viewing or modification by unauthorized persons.

Archive backup procedures

Archives backed up to write-only storage media such as CD-ROMs or DVDs must be periodically refreshed to guard against deterioration and consequent loss of data.

Requirements for time-stamping of records

Archive collection system (internal or external)

Procedures to obtain and verify archive information

Key Changeover

Canadian Pacific internal RPs will normally have the new CA key installed automatically and notifications will be sent out by e-mail at least 30 days prior to CA key changeover.

External RPs will be notified by e-mail at least 30 days prior to CA key changeover.

In either case, the authenticity of the new key may optionally be certified using the old private key.

E-mail notifications will rely on information available to the RA or CA. This will normally consist of information obtained at the time the original End Entity certificate was created.

Compromise and Disaster Recovery

Incident and compromise handling procedures

The CA will use Canadian Pacific’s existing procedures to handle compromise of the CA systems.

Computing resources, software, and/or data are corrupted

The CA will develop procedures to be used in the event of the corruption or loss of computing resources, software and/or data.

Entity private key compromise procedures

In the event of the CA's Digital Signature certificate being compromised, the CA must immediately notify:

- The Chief Information Officer
- The Director of Enterprise Security
- All RAs
- All Subscribers

After addressing the factors that led to the compromise, the CA may generate a new CA signing key pair and re-issue certificates to all Entities, ensuring that all CRLs are signed using the new key.

Business continuity capabilities after a disaster

The CA shall prepare and maintain a business continuity plan outlining the steps to be taken in the event of a disaster.

The business continuity plan should address, at a minimum:

1. Roles and responsibilities
2. The process to be followed before the plan is activated;
3. Activation conditions
4. Fallback procedures
5. Alternative locations
6. Resumption procedures
7. How and when the plan will be tested
8. The process for maintaining the plan
9. Awareness and education activities

CA or RA Termination

If a CA ceases operation or makes a major change in operations, the CA shall provide the Director of Enterprise Security with a list of all issued certificates. The list shall be provided prior to or immediately upon the termination or major change in operations.

In the event the CA ceases operations, the CA shall arrange for the secure retention of the CA's records, including two copies of:

- Certificates
- Private keys
- PINs or passwords required to operate the CA
- CA self-signed certificates
- CRLs
- Audit information

TECHNICAL SECURITY CONTROLS

Key Pair Generation and Installation

Key pair generation

The CA shall ensure that CA key generation shall be:

- Performed by personnel in trusted roles and requiring, at a minimum, dual control
- Carried out within a device which satisfies, at a minimum, the requirements identified in the Section headed "Cryptographic module standards and controls" on page 39, below
- Performed using an approved algorithm

Keys for End Entities other than the CA must be generated using an approved algorithm and may be generated in a software or hardware cryptographic module.

Where a key pair is generated by the CA on behalf of a prospective certificate holder, the CA copy of the key pair must be destroyed in a secure manner following the placement of the keys in the custody of the prospective certificate holder.

Private key delivery to subscriber

A private key generated by the CA for purposes of digital signature shall be made available to the Subscriber in such a manner that only the Subscriber may access it. Any copies of the key made by the CA shall immediately be destroyed in a secure manner.

Private keys generated for data encryption purposes shall be supplied to the Subscriber in a secure manner. A secure copy of the private key shall be kept by the CA.

Public key delivery to certificate issuer

Public keys shall be delivered in a secure manner which will be described in the CPS.

CA public key delivery to relying parties

The CA public key will be delivered to RPs in a secure manner using normally accepted commercial practices.

Key sizes

Root CA and Issuing CA key sizes shall be 2048-bit RSA.

Subscribers may request 1024-bit RSA keys but should be encouraged to use 2048-bit RSA.

Public key parameters generation and quality checking

The Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) algorithm **shall not** be used under any circumstances.

Subject to the stipulation in the previous paragraph, all CA keys must be generated in hardware using a random or pseudo-random number generator that is capable of satisfying statistical tests as well as the cryptographic module requirements in FIPS Publication 140-2, level 3.

Subject to the stipulation in the first paragraph of this sub-section, key pairs for entities not listed above may optionally be generated and stored in software or hardware cryptographic modules.

Key usage purposes (as per X.509 v3 key usage field)

Keys may be used for authentication and data integrity and in support of non-repudiation.

Only CA signing keys may be used for signing certificates and CRLs.

Private Key Protection and Cryptographic Module Engineering Controls

Subscribers are responsible for protecting their own private keys. The private key must be protected using commercially reasonable cryptographic and physical access control. The level of protection must be adequate to deter a motivated attacker with substantial resources.

Encryption private keys must be stored on password protected media, or when stored by the CA protected by cryptographic hardware.

Cryptographic module standards and controls

All CA digital signature key storage and certificate signing operations must be performed in a secure hardware cryptographic module rated to at least FIPS 140-2, Level 3.

Private key (n out of m) multi-person control

There must be multi-person control for CA key generation.

At a minimum, there must be multi-person control such that no single person can gain control over the Certificate Authority (CA) signing key.

There must be multi-person control for Subscriber data encryption private key recovery. Two individuals must participate or be present.

Private key escrow

The private keys of the offline Root CA and any subordinate or issuing CAs may not be escrowed.

Subscriber private keys used for non-repudiation (digital signature) may not be escrowed.

Subscriber private keys used for data security (encryption) may be escrowed.

Private key backup

The CAs must back up CA private signing keys in a secure manner to support business recovery operations.

Private key archival

Refer to the Section headed “Records Archival” on page 35, above.

Private key transfer into or from a cryptographic module

If a private key is not generated in the Entity's cryptographic module, it must be entered into the module in a secure manner.

Private key storage on cryptographic module

Private keys stored in cryptographic modules will be encrypted using whatever methods are natively provided by the supplier of the cryptographic module.

Method of activating private key

Use of a private key must require authenticating with a password at a minimum.

The CA shall ensure that password policy rules are in place to require the use of strong passwords to access any environment where private keys are being handled.

Method of deactivating private key

Private keys must be cleared from memory before the memory is de-allocated.

Disk space where keys were stored must be sanitized before releasing the space.

A cryptographic module must automatically deactivate the private key after a pre-set period of inactivity.

Method of destroying private key

Upon termination of the use of a private key, the holder must securely destroy all copies of the key in computer memory and on storage media. Since keys are required to be held in an encrypted form, the deletion of the file or physical destruction of the storage media constitutes an acceptable method of destroying the private key.

Cryptographic Module Rating

Refer to the Section headed “Cryptographic module standards and controls” on page 39, above for standards and specifications.

Other Aspects of Key Pair Management

Public key archival

Issuing CAs shall retain all generated public keys.

Certificate operational periods and key pair usage periods

Issuing CA private signing keys must expire prior to the CA key that signed the public verification key. If the CA certificate contains a private key usage extension, the expiration date for the private signing key must correspond to the date included in that extension.

Subscriber key validity periods must be appropriate to the intended use of the certificate. In any case, Subscriber keys and certificates must expire prior to the Issuing CA key that signed the Subscriber’s public verification key.

Activation Data

Activation data generation and installation

If activation data is used to protect any CA private key it must be unique, unpredictable and protected by a combination of cryptographic and physical access control mechanisms.

Keys and initialization data may sometimes be generated in bulk and shall be held by the CA in a secure manner prior to distribution. Upon receipt of the digital signature key pair and associated initialization data, a Subscriber must use the initialization data in a timely manner.

Activation data protection

Data used for Entity initialization must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

The activation data must have an appropriate level of strength for the keys or data to be protected. The level of protection must be adequate to deter a motivated attacker with substantial resources. If a password scheme is used, the mechanism shall include a facility to lock the account after a predetermined number of failed login attempts. An Entity must have the capability to change its password at any time.

Other aspects of activation data

Not specified

Computer Security Controls

Specific computer security technical requirements

Computer security controls for CAs must provide protection from unauthorized access, modification, substitution, insertion and/or deletion. The following functionality for CAs must be provided by the operating system, or through a combination of operating system, PKI CA software and physical safeguards:

1. Access control to Certificate Authority (CA) services
2. Enforced separation of duties for Certificate Authority (CA) administrative roles
3. Identification and authentication of Certificate Authority (CA) administrative roles and associated identities
4. Use of cryptography for session communication and database security
5. Archival of Certificate Authority (CA) and End-Entity history and audit data
6. Audit of security-related events
7. Trusted path for identification of PKI roles and associated identities
8. Recovery mechanisms for keys and Certificate Authority (CA) system
9. Archival of CA and End-Entity history and audit data
10. Audit of security related events
11. Automatic and regular validation of CA database integrity
12. Recovery mechanisms for keys and the CA system
13. Hardening of the CA's operating system

Computer security rating

Life Cycle Technical Controls

System development controls

All Canadian Pacific PKIs must use CA software which has been designed and developed under a formal and documented development methodology. Security considerations and formal reviews (including third-party reviews) must be integral to the methodology.

Purchased hardware or software shall be shipped or delivered in a sealed or shrink-wrapped container and be installed by trained personnel.

Security management controls

CA software must provide a method for a CA to verify that the software on the system:

- Is from a traceable source
- Has not been modified
- Is the correct version

For establishment of the Root CA, shrink-wrapped software installation shall be conducted under the scrutiny of at least two observers and the Root CA hardware and software handed over to CP Police for secure chain of custody from that point forward.

Life cycle security controls

A formal configuration management methodology must be used for installation and ongoing maintenance of a CA system.

The CA hardware and software shall be dedicated to performing only CA-related tasks. There must be no other applications, hardware devices, network connections or component software, which are not part of the CA operation.

The CA shall implement policies and procedures to prevent malicious software from being loaded onto the CA equipment.

Network Security Controls

The offline CAs are not connected to a network so this section does not apply to offline CAs

The CA shall ensure that proper controls are put in place to ensure CA integrity and availability through any network with which it is connected. Protection must include installation of one or more devices configured to allow only protocols and commands required for CA operations. Network software must be restricted to the bare minimum necessary to allow the CA to function.

Time-stamping

For Root CAs, system clock time may be readjusted manually by referring to an accurate external time source (e.g. wristwatch). Adjustment of Root CA clock time shall be performed by a minimum of two people and the time adjustment noted in the configuration logs.

For network-attached Issuing CAs, time stamps, where used, must be obtained by reference to a trusted source (e.g. time server).

CERTIFICATE, CRL AND OCSP PROFILES

Certificate Profile

Version number(s)

CAs must issue X.509 Version 3 certificates as described in the IETF *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"* in RFC 3280 and its successors. The PKI software must support all the base X.509 fields as well as any extensions as defined in the Canadian Pacific CPS.

Certificate extensions

The CAs shall publish information regarding any extensions and their restrictions in a location easily accessible to all RPs. Critical private extensions shall be interoperable in their intended community of use.

Algorithm object identifiers

The CAs must use, and RPs must support the following:

- RSA 2048 bit modulus or higher algorithm
- SHA-2 algorithm

The list of algorithms to be used by all PKI Entities may change without requiring the issuance of a new CP or a change in the CP's OID. In the event of any change in approved algorithms, the CA shall ensure that Subscribers and RPs are made aware of the changes.

Name forms

Every DN must be in the form of an X.501 printableString.

Name constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all certificates.

Certificate policy object identifier

A CA must ensure that the Policy OID is contained in every certificate issued.

Usage of Policy Constraints extension

A CA may populate and mark as critical the policy constraints extension.

Policy qualifiers syntax and semantics

A CA may populate the CertificatePolicies extension with the OID and policyQualifiers containing the URL of the CPS. A User Notice Qualifier pointing to an applicable RP Agreement may be used at the discretion of the Issuing CA.

Processing semantics for the critical Certificate Policies extension

CRL Profile

Version number(s)

CAs must issue X.509 Version 2 CRLs as per RFC 4325 "*Internet X.509 PKI Authority Information Access CRL Extension*" and its successors. CRLs must be published on a repository and/or an OCSP responder.

Subscriber and RP software must support the entire base X.509 fields, not including extensions.

CRL and CRL entry extensions

The CPS must define and publish the use of CRL extensions supported by the CAs.

OCSP Profile

Version number(s)

If supported, OCSP responders must implement Version 1 of the OCSP specification as per RFC 2560 "*X.509 Internet PKI Online Certificate Status Protocol*".

OCSP extensions

The CPS must define and publish the use of OCSP extensions supported by the CAs.

COMPLIANCE AUDIT AND OTHER ASSESSMENT

A compliance inspection determines whether the CA's performance meets the requirements established by the Certificate Policy and associated CPSs.

Frequency or circumstances of assessment

A compliance inspection shall be completed at least once every two years.

Identity/qualifications of assessor

The compliance auditor must possess competence in the field of PKI. Additionally, the compliance auditor must be thoroughly familiar with the requirements that Canadian Pacific imposes on the issuance and management of all certificates.

Assessor's relationship to assessed entity

The compliance auditor must not have any financial, legal or conflicting business relationship with the Certificate Authority (CA) that is being audited.

Topics covered by assessment

The compliance audit will cover all requirements that define the operation of a CA under this CP.

Actions taken as a result of deficiency

In the event of a deficiency, the CA shall take commercially-reasonable steps to correct the deficiency. A remediation plan shall be submitted to the Director of Enterprise Security for approval.

Communication of results

The compliance auditor must provide the CA with the results of the compliance audit.

The results will not be made public unless required by law.

OTHER BUSINESS AND LEGAL MATTERS

Subscribers and RPs to this PKI are either employees of Canadian Pacific or external organizations with whom there is an existing, contracted business relationship. The terms and conditions in any employment agreement or inter-organizational agreement will govern the responsibilities of each party and are therefore not specified here.

In general, it is expected that such agreements will, at a minimum, specify terms regarding:

- Fees for various PKI services
- Financial responsibilities to be borne by each party
- How confidential business information must be managed
- Protection of private and personal information
- Intellectual property rights
- Limitation of liability
- Term and termination
- Dispute resolution
- Applicable laws

The CA will take reasonable steps to ensure that there is a pre-existing agreement governing the usage of digital certificates issued by the PKI.