Public release

CENTRE DE CERTIFICATION DU QUÉBEC® (CCQ) PUBLIC KEY INFRASTRUCTURE

CERTIFICATE POLICY

Version: 5.1
OID 2.16.124.113550.1
Approval date: 2019-12-04

Notes

Several changes have been made to this version of the CCQ Public Key Infrastructure (PKI) Certificate Policy, including:

- Change of approver. Now the Board of Directors of Notarius Solutions Inc. will be the one in charge of approving this Certification Policy under the terms of the Resolutions of the Directors of "Notarius - Notarial Information Systems and Technologies Inc." adopted on November 30, 2018.
- Identification of Notarius trademarks by inserting " ® " where applicable.
- Harmonization of definitions according to the recognized terms of ISO (22300) or according to the general conditions of use of Notarius Products.
- Addition of the reference to Notarius' SLAs.
- Integration of the automated approval and revocation process.
- Reminder of the list of acceptable identity verification documents
- Clarification of the Refund Policy, Indemnification & Jurisdiction sections according to the General Conditions of Use of Notarius products
- Addition of sections omitted in the old version (with reference to RFC 3647)
- Deletion of tables that will now be found in CPS.

Governing Language

This English version is a translation of the original French. Should any discrepancy be found between the English and French versions of this CP, the French version will prevail.

Version Tracking

Version	Date	Description	Editor/Collaborators	Approving
2.0	2001-07-16		Liette Boulay, Director Legal Services	Chambre des notaires du Québec
3.0	2003-04-03	PKI legal name change to Quebec Certification Centre	Liette Boulay, Director Legal Services	Chambre des Notaires du Québec
3.2	2005-08-26	Modification of the data retention period to 10 years & addition of a transitional clause	Liette Boulay, Director Legal Services	Chambre des Notaires du Québec
3.3	2006-05-18	Allowing certification services to professionals outside Quebec	Liette Boulay, Director Legal Services	Chambre des Notaires du Québec
3.4	2006-08-17	Abolition of the concept of a basic certificate for notaries	Liette Boulay, Director Legal Services	Chambre des Notaires du Québec
3.5	2007-06-20	Revision to meet ISO 27001 requirements	Liette Boulay, Director Legal Services	Chambre des Notaires du Québec
3.6	2008-02-15	Adjustment for ISO 27001 compliance	Liette Boulay, Director Legal Services	Chambre des Notaires du Québec
4.0	2011-04-07		Liette Boulay, Director Legal Services	Chambre des Notaires du Québec

4.5	2015-07-16	Decision of the CNQ Work's Council of November 14, 2012: The Certification Authority is now the CA of Notarius TSIN inc. The PSC/R is Solutions Notarius Inc.	Liette Boulay, Director Legal Services & Compliance	The Board of Notarius TSIN Inc.
5.0	2018-04-27	Complete redesign for eIDAS compliance	Maud Soulard, PKI Officer Alexandre Provost, IT Team Leader	The Board of Notarius TSIN Inc.
5.1	2019-12-04	Identification of the new approver Adjustment of terms and definitions	Maud Soulard, PKI Officer	The Board of Solutions Notarius Inc.

Intellectual Property

Table of Contents

1 General Provisions

1.1 Overview

The mission of Solutions Notarius Inc. (hereinafter "Notarius") is to provide digital and electronic signature solutions that ensure the long-term reliability of documents.
Notarius has also been a trusted service provider serving professionals and their business partners for many years.

Since 1998, Notarius's Public Key Infrastructure (PKI) known as the Centre de Certification du Québec (CCQ) allows the issuance of keys and certificates for signing electronic documents. For notaries and land surveyors in Quebec, it also provides the encryption of key data.
We can therefore say that:

- The CCQ's digital signature certifies the signatory's professional status or employment affiliation.
- The digital signature's integrity protects the document's content against unauthorized changes.
- Encryption guarantees the origin and integrity of key document data.

This Certificate Policy (hereinafter the "CP") defines Notarius's commitments and undertakings as a provider of qualified and advanced certificates.
This CP complies with the principles and recommendations defined in ETSI EN 319 401, ETSI EN 319 411-1 & ETSI EN 319 411-2 standards.

Certificates issued by the CCQ are used for digital signatures that have the same legal validity as handwritten signatures, and as such are admissible in court subject to their confidentiality or any protection conferred by professional secrecy. These certificates attest to the identity of the natural persons to whom they have been issued when acting as signatories.

Notarius issues certificates to its own employees as well as to clients, companies, organizations, professional associations, and others.

Because Notarius holds several PKIs. The scope of this CP is only limited to the Centre de Certification du Québec (CCQ) (see CPS for details).

1.2 Document Identification and Object Identifier Numbers (OID)

This CP is called the *Centre de certification du Québec (CCQ) Public Key Infrastructure - Certificate Policy*.
It is identified in particular by its object identifier number (OID) as follow: 2.16.124.113550.1

The CP is supplemented by a corresponding *Certification Practice Statement* (CPS), also referenced by an OID number: 2.16.124.113550.1
The Certificate Policy and Certification Practice Statement identified above are respectively referred to as "CP" and "CPS" in the following sections of the document.

The OIDs for the CCQ consist of the following:

- (2) country
- (16) Canada
- (124) Notarius
- (113550.1) Certificate Authority

1.3 Definitions and Abbreviations

1.3.1 Abbreviations

The abbreviations used in the CP are as follows:

- **ARL**: Authority Revocation List
- **AVA**: Affiliation Verification Agent
- **CA**: Certification Authority
- **CISO**: Chief Information Security Officer
- **CCQ:** Centre de certification du Québec
- **C/RSP**: Certification and Repository Services Provider
- **CN**: Common Name
- **CP**: Certificate Policy
- **CPS**: Certification Practice Statement
- **CRL**: Certificate Revocation List
- **CRM**: Customer Relationship Management
- **DN**: Distinguished Name
- **ETSI**: European Telecommunications Standards Institute
- **ISO**: International Organization for Standardization
- **IVA**: Identity Verification Agent
- **LRA**: Local Registration Authority
- **OCSP**: Online Certificate Status Protocol
- **OID**: Object Identifier
- **PKI**: Public Key Infrastructure
- **RA:** Registration Authority
- **RPA**: Recognized Professional Association
- **RPO**: Recovery point objective
- **RTO**: Recovery time objective
- **SLA:** Service Legal Agreement
- **SS**: Self-Service

1.3.2 Definitions

The terms used in this CP have the following meanings:

- **Activation**: Operation performed by the subscriber and consisting of registering activation data using a cryptographic device to generate the subscriber's certificates.
- **Activation data**: Information needed to activate keys and certificates that the subscriber must protect to ensure confidentiality (e.g., a PIN).
- **Attribution**: Issuance of keys and certificates to an applicant.

- **Audit**: An independent monitoring of a system's records and activities conducted by a competent and impartial agent to assess the suitability and effectiveness of system controls, ensure compliance with established operational policies and procedures, and recommend necessary modifications to controls, policies, or procedures.
  Audits assess the management process put in place by the C/RSP or LRA to identify weaknesses and/or nonconformity. Audit findings enable the C/RSP and LRA to take the appropriate actions to correct all observed shortcomings and malfunctions.
- **Authentication**: Process to verify the declared identity of a subscriber (individual or organization) in order to grant the subscriber access to resources (systems, networks, or applications).
- **Automated approval and revocation process**: Service that allows a professional Order to automate the approval stage of applications for professional digital signature applications from its members or the revocation of such applications based on the transmission and processing of data directly from the Order's register provided to Notarius on a daily basis.
- **Business Partner**: A legal person that wishes to perform electronic transactions with subscribers. It must be authorized to do so and have an agreement to this effect in place with the C/RSP.
- **Buyer:** The person who initiates the subscription process for one of Notarius's Products, for himself or for an Authorized Holder.
- **Cancellation**: An action taken by the C/RSP consisting of withdrawing an application to issue certificates prior to their activation, either at the subscriber's request or when the prescribed activation period has lapsed.
- **Certificate and Repository Services Provider (C/RSP)**: Entity responsible for administering certificate and repository services associated with certificate issuance and management.
- **Certificate application:** Message sent by an entity to the CA to request the issuance of a certificate.
- **Certificate Policy (CP)**: A set of rules, identified by an object identifier (OID), setting out the requirements that bind the CA in the implementation and delivery of its services.
- **Certificate Revocation List (CRL)**: A list, digitally signed by a CA, containing certificate identities that are no longer trusted (revoked or invalidated). This list is signed by the CA to prevent modification by an unauthorized person. It includes the certificate date of issuance, date of any updates (both optional), and the CRL itself with two items for each entry: the serial number of the revoked certificate, and the reason for revocation.
- **Certificates**: Sets of information including, at the very least, the minimum provided for in the *Act to establish a legal framework for information technology* (RSQ, c C-1.1), signed by the CA and designed to confirm the subscriber's identity, among other functions.
- **Certification Authority (CA)**: Entity responsible for certificates signed in its name as well as the CCQ. The CA may delegate duties to a third party.
- **Certification Practice Statement (CPS)**: Document that establishes and details the organizational, procedural, operational, technical, and human practices observed by the C/RSP in order to provide certification services in accordance with its binding CP.
- **Client application**: An application or software program installed on the subscriber's workstation or accessed online through which the subscriber can activate or recover certificates, change their password, perform configuration tasks, or make transactions using their certificates.

- **Compromise**: A confirmed or suspected security policy breach in which unauthorized disclosure or loss of control over sensitive information may have occurred. With respect to private keys, a compromise may include the loss, theft, disclosure, modification, or unauthorized use of a private key, or any other event compromising the integrity of a private key.
- **Confidentiality:** Information property that may only be made available or disclosed to authorized individuals, entities, or processes.
- **Customer Relationship Management (CRM)**: A management tool used by the C/RSP to capture, process, and analyze information about clients, partners, employees, or prospects.
- **Device**: Application authorized by the C/RSP that permits the comprehensive or partial management of a subscriber's keys and certificates, including but not limited to their activation, renewal, and recovery. A device may be a software program, transaction platform, or web service.
- **Digital Signature:** the private and public keys contained in a certificate issued to a Holder for the purpose of identifying him/her in the context of his/her use of the Products. Certificates include all information confirming the Holder's identity. Notarius cryptographically links an official identity to the Digital Signature certificate protected by two-factor authentication that is securely delivered to a validated user. Digital Signatures issued by Notarius can be affixed to PDF, PDF/A, and any other type of supported documents. The types of Digital Signatures vary according to the Product(s) to which the user has subscribed. A Digital Signature remains valid until it expires or is revoked.
- **Holder:** An organization, legal entity or natural person that has subscribed to the service (by itself or by a purchaser) and that holds CCQ PKI keys and certificates enabling it to sign, authenticate and/or encrypt according to its needs or available functionalities. The Holder is a duly authorized end user of one of the Notarius products.
- **Integrity**: Refers to the accuracy of information, the source of said information, and the operations of the system that processes it.
- **Issuance:** The act of assigning one or more keys and certificates to an applicant.
- **Key pair:** A key pair is a combination of a private key (to be kept secret) and a public key, both of which are required to execute cryptographic techniques based on asymmetric algorithms.
- **Legal person**: Includes any corporation, company, government agency, or public body and, by extension, a partnership, association or trust. The term "legal person" will be used inclusively to enhance readability.
- **Local Registration Authority (LRA)**: A Recognized Professional Association (RPA) or legal person responsible for performing functions delegated by the C/RSP. LRAs must be bound by a written agreement with the C/RSP.
- **Maximum Data Loss:** Also referred as a Recovery point objective (**RPO**) is the point to which information used by an activity is to be restored to enable the activity to operate on resumption.
- **Modification:** Action performed with the intent to correct the information contained in a certificate by attributing a new, modified certificate.
- **Policy Object Identifier (Policy OID)**: Numerical designation contained in the certificate that refers to the CP and makes it possible to establish the certificate's trust level.
- **Private key**: The key in a subscriber's asymmetric key pair that must be used only by the subscriber.
- **Public key**: The key in an entity's asymmetric key pair that can be made public.

- **Public Key Infrastructure (PKI)**: Set of physical components, functions, and procedures performed by software and human resources to manage keys and certificates issued by the CA.
- **Reattribution:** The attribution of new certificates to the same subscriber following the revocation or non-renewal of their certificates.
- **Recognized Professional Association (RPA)**: A legally constituted professional association expressly dedicated to safeguarding the public interest, with which members of a given profession are affiliated and which enjoys government-sanctioned prerogatives such as regulatory and disciplinary powers. All professional associations and orders governed by Quebec's *Professional Code* are deemed RPAs.
- **Recovery**: Action performed at the request of the subscriber or the C/RSP to regenerate the subscriber's keys and certificates when they cease to function, particularly due to a technical problem, the accidental destruction of a user's profile, or a forgotten password.
- **Recovery time objective (RTO):** Period following an incident within which a product or service or an activity is resumed, or resources are recovered.
  For products, services and activities, the recovery time objective is less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable
- **Registration Authority (RA):** an entity that verifies that applicants or certificate holders are identified that their identity is authentic and that the constraints associated with the use of a certificate are met.
- **Relying Party**: Any person who relies on a certificate issued under the CCQ. A Relying Party may also be a CCQ certificate subscriber.
- **Renewal**: A procedure automatically performed prior to the expiry date of a valid certificate to generate a new certificate for the subscriber.
- **Revocation**: The withdrawal of a subscriber's certificate performed at the discretion of the C/RSP or at the request of an authorized individual.
- **Self-Service (SS)**: The Notarius digital signature management platform.
- **Shared secret or security questions**: A word or groups of words shared securely between the C/RSP and the subscriber so that the subscriber can be remotely identified.
- **Subscription:** The subscription to one or more Notarius Products to which the Holder or the Purchaser/Buyer has subscribed.
- **Subscription Fees**: The Subscription Fees that the Purchaser/Buyer must pay annually or monthly, as the case may be, for use by a Holder of one or more Products, in addition to the Membership Fees and Transaction Fees.
- **Subscriber:** Any organization, legal person, or individual that has subscribed to the service and holds PKI keys and certificates allowing them to perform signing, authentication, and/or encryption tasks as per their needs and available functions. Subscribers can hold certificates that may be assigned to a group, device, or application.

1.4 Interpretation

This CP constitutes a "policy statement" within the meaning of section 52 of the *Act to establish a legal framework for information technology* (R.S.Q., chapter C1-1).

1.5 Compliance with Applicable Standards

This CP meets applicable industry standards, including eIDAS and ISO 27001.
It sets out Notarius's commitments as a supplier of trust services, in accordance with ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 standards.
For enhanced clarity, the structure of this CP is based on RFC 3647 *(Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*).[1]

1.6 CCQ PKI Components

1.6.1 Certification Authority (CA)

Notarius, through its Board of Directors, acts as a Certification Authority (CA).
In this role, Notarius undertakes to:

- Issue certificates in compliance with the CP;
- Adopt the proposed amendments to the CP;
- Identify the C/RSP;
- Approve agreements with the C/RSP concerning services offered;
- Negotiate reciprocal agreements with other CAs or CSPs as needed;
- Publish the Certificate Revocation List (CRL) and the Authority Revocation List (ARL).

1.6.2 Certificate and Repository Services Provider (C/RSP):

The CA has appointed the Notarius Executive Committee as the C/RSP.

This Executive Committee is composed of the President and Chief Executive Officer; Vice President, Finance and Administration (also the PKI Officer); Vice President, Sales and Business Development; and Vice President, Operations and Product Strategy.

The C/RSP is responsible for the day-to-day administration of certificate services associated with issuing and managing certificates.

It also acts as the Registration Authority (RA).

The C/RSP has the following responsibilities:

- Propose updates to the CP for approval by CA;
- Develop and update the CPS in accordance with CP requirements;
- Identify and nominate the principal actors of the CCQ, including the PKI Officers and IVA;
- Oversee the administrative and technological aspects of certificate issuance;
- Perform subsequent operations pertaining to the certificate life cycle;
- Provide repository services to confirm the validity of certificates in accordance with CA requirements;

[1] *The X.509 standard defines the formats of public key certificates, certificate revocation lists, and certificate attributes. (Wikipedia.org)*

- Ensure that the necessary verifications have been performed prior to confirming all information contained in certificates;
- Collect and record subscriber information;
- Ensure that the CA publishes CRLs, ARLs, and subscribers' public certificates;
- Ensure that the CA's private key is used exclusively to sign subscribers' certificates, CRLs, and ARLs;
- Implement the necessary measures in accordance with best practices to ensure the security of repository services;
- Store cancelled certificate numbers and associated information;
- Provide support to subscribers;
- Delegate certain functions to the designated Local Registration Authorities (LRAs).

1.6.3 Local Registration Authority (LRA)

1.6.3.1 Definition

The Local Registration Authority (LRA) is responsible for performing all functions delegated to it by the C/RSP.

The LRA may be a Recognized Professional Association (RPA), such as a professional association or order, or a legal person.

1.6.3.2 Signing Contractual Agreements

All LRAs have signed contractual agreements with the C/RSP or with one of its representatives that is has delegated and authorized to do so.

1.6.3.3 Roles and Responsibilities of LRAs

The LRA formally delegates its authority to Affiliation Verification Agents (AVAs) for businesses or professionals that it has expressly identified to the C/RSP.

The LRA must:

- Always have at least two persons (or one person in the case of legal persons) to act as an Affiliation Verification Agent (AVA), and take all actions necessary to comply with this requirement;
- Ensure the management of AVA appointments;
- For each business day, ensure that at least one (1) AVA is available, trained and ready to approve or revoke the digital signatures of employees or members of the LRA or to deal with exceptions to the automated verification of membership status in cases where the LRA is a Association/Order that has adhered to the Automated Approval and Revocation Process;
- Ensure that AVAs complies with all obligations set out in the CP;
- Ensure that the information on the Association/Order's register (or Registry of Members) is always up-to-date and error-free when it has decided to join the Automated Approval and Revocation Process.

The LRA or its AVA must:

- Apply and comply with the CP and all established procedures for using the management portal, where applicable;
- Approve or reject the registration of initial certificate applications submitted to it by confirming the applicant's registration on the roll of their professional association or order (and the accuracy of all information provided concerning the applicant's name) or that the applicant is employed by the LRA;
- Revoke the professional digital signature of any Holder who no longer meets the requirements of their Professional Association or Order;
- Request that the C/RSP revoke, when necessary, the corporate digital signatures of its employees on its corporate account;
- Unless otherwise contractual agreement, act as the front-line point-of-contact for all subscribers it manages.

1.6.4 Holder

1.6.4.1 Definition

A CCQ PKI key or certificate holder is a natural person, group or application that uses its certificate to sign, encrypt (*members of the Chambre des notaires du Québec (CNQ) and the Ordre des arpenteurs-géomètres du Québec (OAGQ) only*) and/or authenticate itself according to its needs or the functions available to it.

1.6.4.2 Roles and Responsibilities

Subscribers must:

- Comply with all applicable terms and conditions of this CP;
- Respects the General or Specific Conditions of Use of Notarius products available at all time on its website;
- Fulfill the subscription requirements;
- Provide all information and documentation required;
- Protect the confidentiality of their activation data, authentication data, password, and private key and the equipment or media on which it is stored;
- Ensure that they are the only ones to use their certificates or, when they are assigned to a group, device or application, to ensure that they are only used by authorized persons and systems;
- Use their certificates for the authorized purposes only;
- Sign documents online to ensure their authenticity;
- Use all computer equipment in a secure manner;
- Notify the C/RSP customer service as soon as possible if the Subscriber suspects that the confidentiality of their keys and certificates, or their password(s), is compromised;
- Notify the C/RSP as soon as possible of any changes, or make such required changes to their account itself, through the Self-Service option;
- Refrain from using certificates the moment they are revoked or expired.

1.6.5 Other Participants

1.6.5.1 Business Partners

A Business Partner is defined as a legal person that wishes to deal electronically with certificate holders. It must be authorized to do so and have entered into an agreement to this effect with the C/RSP.
The Business Partner must:

- Align its business processes with the use of CCQ PKI keys and certificates;
- Comply with all technical and functional requirements stipulated by the C/RSP;
- Designate a person within their organization to hold CCQ PKI keys and certificates;
- Manage user access and permission for its IT applications;
- Ensure that all necessary updates reflect changes to the CCQ PKI;
- Inform subscribers of authorized uses of its applications;
- Ensure that subscribers are equipped to comply with all obligations arising from the Policy, including but not limited to the obligation to maintain the confidentiality of private keys;
- Notify the C/RSP of any event that may require action to be taken on keys and certificates, including their revocation.

The C/RSP may, at its discretion, require the Business Partner to undergo an audit or provide an audit report.

1.6.5.2 Third-party Users

A third-party user is a person who acts based on a certificate issued under the CCQ PKI.
A third-party user may or may not be a CCQ PKI key or certificate subscriber/holder.
Any third-party user wishing to act based on a certificate must ensure that the certificate:

- Has been issued by the CCQ PKI;
- Meets the required trust level;
- Has not expired;
- Has not been revoked.

1.6.5.3 The person authorized by the Chambre des notaires du Québec (CNQ)

It is a notary who is a member in good standing of his Professional Order (non-Class C), who has been authorized by the PSC/R and the CNQ to verify the applicant's identity and who must confirm this verification of identity to the CNQ according to established exceptional procedures.

1.7 Use of Keys and Certificates

1.7.1 Authorized Use of Keys and Certificates

Certificates issued under this CP can be used for the purposes stipulated in the certificate itself, specifically in the “key usage” or “extended key usage” field.

Depending on the product chosen, holders can use keys and certificates for one or more of the following purposes:

- To confirm their identity;
- To authenticate their identity using authorized services or platforms;
- To digitally sign electronic documents to ensure their integrity and non-repudiation;
- For Quebec notaries and land surveyors only, encrypt electronic documents to ensure confidentiality of information.

All subscribers and third-party users must assess the circumstances and associated risks before deciding whether or not to use a certificate issued under this CP.

The table below specifies the digital signatures in the CertifiO® range and provides a brief description of the appropriate uses of those products.
These descriptions are for information purposes only; they can also be found on our website at www.notarius.com.

Product/Certificate Type	Appropriate Use
CertifiO for Professionals	Digital signature certificate, certifying the identity and professional status of the signer. For the exclusive use of the professional named in the certificate. The professional's membership number is indicated in the certificate. Requires an agreement between Notarius and the subscriber's professional association or order. Face-to-face identity verification with the IVA of the C/RSP (or in front of the authorized sponsor for notaries in Quebec). Certification of employment status or employment relationship.
CertifiO for Employees	Digital signature certificate, certifying the identity and relationship with the employer. For the exclusive use of the individual named in the certificate. Face-to-face identity verification with the IVA of the C/RSP. Also certifies the employer's name.
CertifiO for authentication to the systems of Registre Foncier (SIRF)	Digital Signature Certificate for the exclusive use of the individual named in the certificate. SIRF individual digital signatures are used specifically for authentication with the Quebec Land Registry Systems online. Face-to-face identity verification with the C/RSP IVA.

1.7.2 Limitations of Use

The CA and C/RSP may restrict the use of keys and certificates provided that affected signature holders are expressly notified.
The subscription agreement, the general or particular conditions of use of Notarius products or specifications of a product may limit the uses that the holder of its certificates may make.

As certificates are used solely at the subscriber's discretion, certificate use does not constitute a warranty as to the subscriber's reputation or trustworthiness or guarantee that the subscriber's use of the certificate will comply with applicable laws and regulations. Subscribers are, however, bound to strictly adhere to the authorized uses of keys and certificates. Subscribers failing to do so may be held liable.
Finally, subscribers undertake not to use certificates that have been revoked or expired.

1.7.3 Authorized Holder

The authorized holder is:

- A member of an RPA who has an agreement with the C/RSP;
- An individual acting for a Legal Person (employee, agent, etc.) who wishes to use keys and certificates for professional purposes on behalf of that Legal Person;
- Any individual who wishes to have a certificate for their own use and who meets the requirements of the C/RSP;
- A natural person who wishes to deal with the Québec Land Register online.

1.8 Policy Administration

1.8.1 Organization Administering the Document

This CP is under the responsibility of Solutions Notarius inc.

1.8.2 Contact Person

Any questions or comments regarding this CP, the certificates issued by the CA or any disputes should be addressed to:

Solutions Notarius Inc.
Attn: General Management
465 Rue McGill, Suite 300
Montreal, QCH2Y 2H1
Phone: 514-281-1577
Email: Officiers@notarius.com

1.8.3 CP and CPS Approval Procedures

The Solutions Notarius Inc. Board of Directors (hereinafter the "Board") is responsible for approving this CP on behalf of Notarius.
Solutions Notarius Inc. determines CPS compliance with the CP through its Executive Committee.

The CPS is deemed compliant with the CP through an approval process by the members of Notarius's Executive Committee. If the Notarius Board approves changes to the CP, the PKI Officer revises the CPS accordingly.

CPS updates are implemented only after they have been approved and are published on the Notarius website.

2 Publication and Repository Responsibilities

2.1 Repositories

The C/RSP is responsible for making available and publishing via its website of the CP and the general and specific terms and conditions of use of its products as well as its RTOs, RPOs via its SLAs.
It also makes information on the revocation status of valid certificates issued by the CA available to users and user applications.
Delivery methods and addresses are specified below.

2.2 Publication of Certification Information

The information publicly disseminated by the C/RSP for the CA is:

- The CP (https://notarius.com/en/certification-policy/)
- The CPS (coming soon in english)
- The General and specific Terms of Use for products offered by Notarius (https://notarius.com/en/legal-info/)
- Service Level Agreements including its RPOs and RTOs (https://notarius.com/en/legal-info/#conditions_sla)
- Certificate application forms (https://notarius.com/en/products/certifio/)
- The Root CA certificate
- Valid and up-to-date CRLs:
  - http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl
  - http://webcrl2.notarius.net/crl/ccq_combined_crlfile1.crl
- ARLs:
  - LDAP://cn=CRL1,ou=AC1,o=CENTRE DE CERTIFICATION DU QUEBEC,c=CA

2.3 Time and Frequency of Publication

Information related to the Notarius CCQ PKI is published as necessary to ensure published information always remains consistent with the CA's current commitments, methods, and procedures.

The deadlines and frequencies for publishing information on the status of certificates, and the availability requirements of the systems publishing them, are described below:

- The Root CA certificate is published as soon as possible after its issuance, and must be released prior to any release of the corresponding CRLs;
- The CRL is updated and published at least every two (2) hours;
- The CRL validity period is a maximum of forty-eight (48) hours;
- The CP and the CPS are published on the Notarius website as soon as possible after their adoptions. They are therefore available 24 hours a day, 7 days a week;
- The CP updates are clearly identified in the "News" section of the Notarius website;

- If applicable, professionals who are directly affected by changes to the CP will be notified by email in respect of existing contractual agreements;
- The publication of a certificate status by the C/RSP constitutes a notice to third-party users. For this reason, a certificate must be considered revoked by third-party users as soon as this information is published;
- The general and specific terms and conditions for the use of Notarius products are published on its website, as are the SLAs. They are therefore available 24 hours a day, 7 days a week.

2.4 Access Controls on Repositories

All information published for certificate signature holders is freely accessible for reading.
The CP, CPS, General and Specific Terms of Use and CRL are available on the Notarius website and can be read by anyone who wishes to do so.
The ability to modify content in publishing systems (add, delete, or modify published information) is restricted to those holding authorized positions in the CCQ PKI through strong controls (based on at least two-factor authentication).

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

To identify a signature holder, the certificates issued follow identification and name rules. The certificates issued by the CA therefore comply with the specifications of X.509 Version 3 .
Consequently, in each certificate, the issuing CA (Issuer) and the signature holder (Subject) are identified by a unique "Distinguished Name" (DN) or by a "Unique ID" ("UID") in X.501 form.

3.1.2 Explicit Names

Names chosen to designate the certificate holders must be meaningful.
The UID/DN is presented in one of the forms below, depending on the product the user has subscribed to.

<table>
<tr><th>Product</th><th>Serial number</th><th>CN (Common Name)</th><th>OU =</th><th>O =</th><th>C=CA</th></tr>
<tr><td>CertifiO for Professionals</td><td>Membership number</td><td rowspan="3">Contact first and last name</td><td rowspan="2">Name in the DN of the account
or
Account name
or
LRA'S name
or
CORPORATION</td><td rowspan="3">CENTRE DE CERTIFICATION DU QUÉBEC</td><td rowspan="3">C=CA</td></tr>
<tr><td>CertifiO for Employees</td><td>Professional email address
The @ replaced by parentheses before and after the domain</td></tr>
<tr><td>SN SIRF</td><td>Professional email address

The @ replaced by parentheses before and after the domain</td><td>CLIENTS</td></tr>
</table>

3.1.3 Anonymization or Use of Pseudonyms

The CP does not allow the use of pseudonyms in its certificates.

3.1.4 Rules for Interpreting Various Name Forms

Names chosen to designate certificate holders must be meaningful;
Distinguished Names (DNs) contained in the "Subject – DN" field of certificates are interpreted according to X.501 and RFC 3280.
The names used in the "Common Name" (CN) field of certificates are the contact first and last name.

3.1.5 Uniqueness of Names

The uniqueness of the DN is guaranteed by using a combination of identification elements (see table

above).
A DN assigned to one signature holder cannot be reassigned to another; this applies for the entire lifetime of the CA.

3.1.6 Identification, Authentication and Role of Trademarks

For trademarks, corporate names, and other distinctive signs, Notarius performs no prior art search or other verification; applicants are responsible for ensuring that the name requested does not infringe on the property rights of any third party.

3.2 Identity Validation

Notarius refers to NIST (800-63A) as a frame of reference for identity verification, particularly in relation to the reliability of the documents presented ("Superior", "Strong" or "Fair"). See details in the CPS.

The identity of an applicant is verified by an authorized person.

The rules and acceptable means for establishing an applicant's identity and, where applicable, its affiliation with an RPA or legal person, are detailed in the CPS.

3.2.1 Initial Identity Verification

The initial identity verification is required:

- To establish the identity of a natural person;
- To validate the identity of a legal person and its relationship with the natural person.

The initial verification of the identity of a natural person requires the presentation of 2 supporting documents such as valid official documents from a recognized government authority.
The primary document presented must include the applicant's given name(s), surname(s), date of birth, photograph and signature. The second or third document (if required), which serves to increase confidence and not to ensure accuracy, should include at least the given name(s) and surname(s). See CPS for details.

Identity-related information about the applicant that is included in the certificate must match the information presented as part of the IVs, to that on the membership form or to that on the roll of the professional order for CertifiO for Professionals signatures.

Except for the notaries, for whom only authorized respondents from the PSC/R and the CNQ are required to conduct the Identity verification in person, the initial application for keys and certificates always requires a face-to-face or a videoconference verification of the applicant's identity (individually or in a group session) by the C/RSP' authorized IVA.

Where technological resources permit and in compliance with ETSI EN 319 411-1, section 6.2.2, verification of the identity of the holders for the issuance of a second digital signature certificate can also be completed by means of their first certificate, issued in accordance with the initial identity verification process explained above. The phases of this process are also detailed in the CPS. This does not apply to members of the CNQ.

Once the applicant's identity has been verified, their affiliation with an RPA will be required where applicable; if so, membership must be confirmed by the RPA concerned via the AVA or via the Automated Approval and Revocation Process.

3.2.1.1 Identity Verification (IV) by an Authorized Agent

To be considered as an authorized agent, the natural person must be:

- The IVA of the C/RSP;
- A notary who is a member in good standing of his or her professional Order (except Class C) and who has been formally designated and authorized by the C/RSP and the CNQ.

Identity verification requires the completion of the specified form and the submission supporting documents (see above).
Identity verification is usually performed by the C/RSP's authorized IVA using videoconferencing or in person by the notary respondent, in accordance with a process described in the CPS.

Note: The recordings of the IV process made by the C/RSP's IVA, including copies of the identification documents, are encrypted and saved in a restricted access environment. Only PKI Officers appointed by the C/RSP have access to these encrypted files.

3.2.1.2 List of Accepted ID Documents

The supporting documents, one (1), two (2) or three (3) as detailed in the CPS, must be valid and issued by a recognized government authority.

The main document submitted must include the applicant's given name(s), surname(s), date of birth, photograph and signature. The second or third document (if required), which serves to increase confidence and not to ensure accuracy, should include at t least the applicant's given name(s) and surname(s). See CPS for details.

The accepted documents are listed in the CPS and on the Notarius website.

3.2.1.3 Affiliation Verification by an Authorized Entity

The RPA or a legal person party to a written agreement with the C/RSP must conduct the affiliation verification.

- Confirmation (manually or through the automated approval and revocation process) of the applicant's affiliation by an RPA is deemed to mean that the applicant is a member in good standing of its professional association or order, or an authorized employee of said RPA and is authorized to hold a digital signature .
- Confirmation of the applicant's employment relationship by a legal person is deemed to mean they are authorized to hold keys and certificates bearing the name or acronym of said legal person.
- Payment of the applicant's subscription fees by a legal person is deemed to be a confirmation of affiliation or employment relationship.

3.2.1.4 Interoperability Criteria

The CA is not party to mutual recognition agreements with any CA outside its security domain.

3.2.2 Identity Validation for Delivery of Activation Data

Activation data used to generate the holder's certificate is delivered to the holder in a way that ensures the identity of the holder and the exclusive use of the activation data.

3.2.3 Identity Validation for Certificate Renewals

The certificate is updated automatically.
The holder will receive a confirmation email in case of successful update.If the automatic renewal process fails, the holder will be notified by email that the update did not work. The holder will then have to recover the certificate by authenticating using t his keys and certificates on the C/RSP Portal.

3.2.4 Identity Validation for a Re-key

When a person requests the re-issuance of its keys and certificates within twelve (12) months of their revocation, expiration, or cancellation, they must successfully authenticate their identity (using its security questions or other valid digital signatures where technology permits) on the C/RSP Portal.
Failing this, applicants will be required to have their identity revalidated in accordance with the procedure described in section 3.2.1.

3.2.5 Identity Validation for Certificate Modifications

When holders wish to change information contained in their certificate, they must successfully authenticate themselves (using its security questions or other valid digital signatures where technology permits) on the C/RSP portal, prior to making the changes themselves. Fields that may be changed by the subscriber are title, work email, other email, phone number, country, and province.

For any other changes not authorized through the C/RSP portal, the holder must contact the C/RSP's client services department to submit a request for the changes to be made on their behalf.

Updating information such as first and last name(s) requires prior verification with the applicant's RPA, which must provide written confirmation of the requested changes. Upon receipt of written confirmation from the RPA, the C/RSP's officer will then make the requested changes.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Natural persons (Buyers) may initiate the subscription process and request keys and certificates for themselves or for an Authorized Holder.
A legal person may apply for keys and certificates for its employees.

4.1.2 Application Process

The Buyer who wishes to obtain keys and certificates must for himself or for an authorized holder must:

- Apply to the C/RSP via the forms provided for this purpose in:
  - Entering signature holder information
  - Entering the buyer's information (if different)
- Verifying the information entered and choosing a payment method.
- Accept the general terms and conditions of the product.
- Pay all related fees.
- Have the identity of the holder verified as described in section 3.2.
- Comply with any other obligations expressly brought to its attention by the C/RSP.

See CPS for details.

4.1.3 Approval or Rejection of Certificate Applications

Upon receipt of a request, once identity verification has been completed, manual or automated validations are made (verification and consistency check of supporting documentation provided) by the C/RSP or the LRA, which must then accept or reject the application. In all cases, the applicant is notified of the decision to use the information provided during the application process.

4.1.3.1 Approval or Rejection of a Corporate Digital Signature Application

Applications for corporate signatures must be approved or rejected by the LRA's AVA, upon receipt of an email that the C/RSP automatically generates.
Confirmation of the employment or the refusal of the request generates an automatic notification for the C/RSP Officer.
Subscription applications are ultimately processed by the C/RSP Officer upon receipt of confirmation of the employment relationship via the restricted-access Notarius digital signature management platform.

4.1.3.2 Acceptance or Refusal of other Types of Digital Signature Applications

Subscription applications are processed either manually by an RPA's AVA via the restricted-access Notarius digital signature management platform or automatically via the automated approval and revocation process.

4.1.3.3 Decisions That Can Be Made Via the C/RSP Management consol

Three (3) types of decisions can be made:

1. **Approve**: Approval of the selected application, as is.
2. **Approve with changes:** Approval of the application subject to changes made to the first name, last name, and/or, where applicable, membership number or professional title.
3. **Reject**: Reject the selected application, providing a reason (mandatory field).
    - An email with the reason for rejection is immediately sent to the applicant.
    - If the applicant has paid by credit card, a refund is credited.
    - A refund is credited to the buyer when he has made the payment by credit card.

4.1.3.4 Decisions That Can Be Made through the Automated Approval and Revocation Process

Two (2) types of decisions can be made:

1. **Approve**: Approval of the selected application, as is.
2. **Reject**: Reject the selected application, providing a reason (mandatory field).
    - An email with the reason for rejection is immediately sent to the applicant.
    - A refund is credited to the buyer when the buyer has paid by credit card.
    - In the case of a mismatch between the nominative information in an application and information contained in the professional Order's table, the buyer will be invited to contact the C/RSP customer support or the AVA of the RPA.

4.1.4 Time to Process Certificate Applications

An application remains valid for a maximum of sixty (60) days while pending acceptance or rejection. After 60 days, the application is deemed null and void, and must be started again.

4.1.5 Certificate Acceptance

Subscribers will be notified by email once their application has been accepted.
The subscriber can then activate their digital signature once the certificate has been generated.
The subscriber is deemed to have accepted the keys and certificates upon activation.

4.2 Certificate Renewal Requests

The certificate renewal operation is independent of the expired certificate.
The renewal service also entails automatic client notifications when the private key is used in a device.
A renewal consists of issuing new keys and certificates to the same subscriber using their existing private key.
During the renewal process, no new identity validation is required.
The issuing CA can renew keys and certificates provided that:

- The original certificates have not been revoked;
- The existing private key is valid and operational;
- The information contained in the certificates has not changed.

No additional validation or verification is necessary.

4.2.1 Who May Request a Renewal

The certificate renewal process can be initiated by:

- An application;
- A device;
- The subscriber using their private key.

4.2.2 Certificate Renewal Procedure

Depending on the applicable *certificate policies*, certificates issued by the CA may be valid for 24 months, 36 months, or longer, calculated from the date of issuance.

The renewal process begins once a certain percentage of the certificate's validity period has elapsed (information also available in the *certificate policies*).

The process is initiated automatically by the subscriber when using their private key on a device.

4.2.3 Processing Certificate Renewal Requests

The certificate renewal processes are initiated automatically by the holder 30 days prior to the key's expiration date, when they use their digital signature online.

For a certificate renewal, it is necessary to:

- Authenticate the subscriber using their private key;
- Generate keys and certificates signed by the CA and send them to the subscriber.

4.2.4 Renewal Notice

Four (4) renewal notices are emailed to the holder at scheduled times. A record of these notices are kept in the contact's file.

The subscriber is notified by the device the moment the certificate is generated.

4.3 Certificate Recovery

Recovery consists of issuing new keys and new certificates while the existing private key is valid but non-operational, especially in cases where the password for the private key has been lost or the keys destroyed.

The issuing CA can renew keys and certificates provided as long as:

- The existing private key is valid;
- The signature holder can authenticate their identity with the C/RSP;
- The information contained in the certificates has not changed.

4.3.1 Who May Request a Recovery

The issuing CA may accept a recovery request initiated by signature holders themselves or by a person in a trusted role (see section 5.2.1).

4.3.2 Procedure for Certificate Recovery

There are different types of recovery procedures:

- Online;
- In person.

4.3.3 Processing a Certificate Recovery

The process is initiated by the certificate holder, by authenticating their identity on a device allowing them to perform the recovery.

Otherwise, the process must be initiated by a person in a trusted role; the certificate holder then receives a notification and the instructions required to perform the recovery using an appropriate device.

4.3.3.1 Online Recovery

Online recovery is a process initiated by the certificate holder via the SS interface platform (with online identity validation).

4.3.3.2 In-person Recovery

In-person recovery involves repeating the application process for a digital signature subscription (see 4.1).

4.4 Certificate Modification Requests

A modification consists in making changes to the information contained in the certificate, provided the existing private key is still valid and operational.

4.4.1 Who May Request Certificate Modifications

The process is initiated by the signature holder or a person in a trusted role (see section 5.2.1). The signature holder then receives a notification and the instructions required to confirm the changes made.

4.4.2 Circumstances for a Modification

A modification can be made to correct a spelling error or change noncritical information contained in the certificate.

4.4.3 Processing Certificate Modification Requests

Holder can modify certain non-critical information contained in the certificate himself. To do so, the holder must first authenticate using his secret questions to the SS interface and make the changes himself.

Otherwise, the holder must send a written request for modification to the C/RSP so that the requested modification(s) can be made on the holder's behalf or transfer the request to the LRA AVAs for approval of the amendment request

4.4.4 Notification of Modifications

Holders must use their private key on a device to receive notifications and view the changes made.

4.5 Certificate Revocation

4.5.1 Circumstances for Revocation

4.5.1.1 Signature Holder Certificates

Revocation consists of rendering a signature holder's keys and certificates unusable and adding the serial numbers of their certificates to the CRL.

Recording this information on the CRL indicates to Relying Parties that the certificate life cycle has

come to an end.
The following circumstances may result in the revocation of a signature holder's certificate:

- The certificate has been rendered obsolete due to a change to the client data contained in it;
- The client information contained in the signature holder's certificate ceases to accurately represent their identity or the intended use of the certificate, prior to the normal certificate expiration date.
- The subscriber fails to comply with the certificate's applicable terms and conditions.
- The client, LRA, RPA, or CA fails to fulfill their obligations under the CP;
- A major error (intentional or unintentional) is identified in the subscriber's account information;
- The subscriber's private key is compromised or suspected of being compromised, or lost or stolen (potentially including associated activation data);
- The subscriber or an authorized person requests the revocation of the certificate (particularly in the event of destruction or damage to the subscriber's private key);
- The CA's signing certificate is revoked (resulting in the revocation of all certificates signed by the corresponding private key);
- The holder does not accept the updated terms of use applicable to the product to which he has subscribed;
- The subscriber dies, or the employer ceases to operate;
- The subscriber is no longer a member in good standing of a professional association or order (a condition of certificate issuance);
- Termination of the contractual relationship between the CA and the LRA and also with holders prior to the end of the validity of the certificates.

The CA or the C/RSP may, at its discretion, revoke a certificate when the holder fails to comply with the obligations set out in the CP. However, this does not apply to digital signature certificates issued to notaries where the approval of the Secretary of the Order is required.

4.5.1.2 CCQ PKI Participant Certificates

Various circumstances may result in the revocation of a certificate held by a particular CCQ PKI participant (including a CA signing certificate used to produce certificates and the CRL):

- A suspected or confirmed compromise, loss, or theft of the participant's private key;
- The decision to change the CCQ PKI upon discovery that one or more participant procedures are non-compliant with the CPS (e.g. following a negative result in a qualification or compliance audit);
- The cessation of activities of the participant's operating entities.

4.5.2 Who Can Request a Revocation

4.5.2.1 Signature Holder Certificates

The following persons or entities may request the revocation of a signature holder's certificate:

- Signature Holders themselves;
- The CA that issued the certificate, or a member of its personnel;
- The LRA or the RPA.

As soon as a person or entity becomes aware of potential grounds for certificate revocation in an area under its responsibility, it must immediately submit a revocation request.

4.5.2.2 Root and Subordinate CA Certificates

The decision to revoke a Root CA certificate may only be made by the CA's Board of Directors, or by judicial authorities through a court ruling.
The revocation of subordinate CA certificates is decided by the entity operating the subordinate CA, which must then immediately inform the Root CA.

4.5.3 Who May Revoke Signature Holder Certificates

The following persons are authorized to revoke certificates:

- Holder themselves;
- Authorized representatives of the RPA, for professional signatures manually or via the dedicated automated approval and revocation process;
- C/RSP officers.

4.5.4 Revocation Request Procedure

4.5.4.1 Revocation of Signature Holder Certificates

The revocation request is submitted to the issuing CA and is signed with the certificate used to make the request.
Revocation requests are processed as a matter of urgency, within a maximum of 24 hours of receipt.
A maximum of five (5) minutes may elapse between the processing of the revocation request and the publication of a new CRL that reflects the processed request.
Details on specific process steps are described in the CPS.

4.5.4.2 Revocation of CCQ PKI Participant Certificates

The CPS specifies the procedures to be implemented in the event of the revocation of CCQ PKI participant certificates.
When any certificate in the certificate chain is revoked, the CA must inform, as soon as possible and using any available means (and, whenever possible, in advance), all affected clients whose certificates are no longer valid.

4.5.5 Notice of Revocation

The subscriber will receive notice of revocation as soon as the operation has been performed if the certificate has been activated.
If the revoked certificate has never been activated, the subscriber will not be notified. A record of the operation will, however, be left in the client file.
When any certificate in the certificate chain is revoked, the CA will inform, as soon as possible and using any available means (and in advance, if possible), all affected users whose certificates are no longer valid.

4.6 Certificate Suspension

Certificate suspension is not permitted under the CP or the CPS.

4.7 Certificate Status Information Functions

The CA provides its third party certificate users with the information necessary to verify and validate the certificate status, including the entire chain of trust.

This certificate status information is available 24 hours a day, 7 days a week.

4.8 Sequestration of Keys and Escrow

The sequestration of private keys is prohibited.

An escrow contract is signed by the CA in the event of the cessation of its operations.

5 Facility Management and Operational Controls

The C/RSP undertakes to implement and maintain the required level of physical security for CCQ PKI participants' operating sites.

5.1 Physical Controls

The CP describes the measures that must be put in place by the C/RSP to ensure the physical security of the CCQ PKI. Specifically, the CP covers physical access controls, protection in the event of a natural disaster, disruption of utilities, and protection against fire, theft, and flood. Controls must be implemented to prevent loss, damage, interruption of business activities, or a compromise of information assets; procedures must also be specified for resuming business after an incident. The requirements described below are minimum requirements. For a more detailed description, see the CPS.

5.1.1 Site Location

The C/RSP ensures that critical and sensitive information is located in secure areas. Planned protective measures should be proportional to the risks identified in the risk analysis.

The CCQ PKI's computer systems are housed in facilities located several kilometres away from one another geographically.

These sites comply with applicable regulations and standards, and meet requirements to ensure the physical security of the building periphery, perimeter, and interior, and specifically those pertaining to:

- Power and air conditioning;
- Exposure to water damage;
- Fire prevention and protection.

These measures also make it possible to uphold commitments made in the CP and in contractual agreements with clients regarding service availability.

5.1.2 Physical Access

All CCQ PKI facilities are controlled and monitored to ensure only authorized persons can access systems and data.

Any person not authorized to access a secure area must always be accompanied by an authorized employee.

Outside business hours, enhanced security is provided using physical and logical intrusion detection systems.

In addition, an access control system for entering and exiting the building is always used during non-working hours.

All entries into and exits from the secure area are independently monitored.

All unauthorized personnel must always be accompanied by an authorized person. All entries and exits are recorded.

In order to ensure the availability of systems, access to machines is restricted to persons expressly authorized to perform operations requiring physical access to said machines. For this purpose, the relevant CCQ PKI participants must define a physical security perimeter where the machines are installed. Doors are controlled by an access control system. Root CAs operate in a space physically isolated from other operations. Access controls for Root CA premises must allow access only to

individuals authorized to access Root CA keys.
See CPS for details.

5.1.3 Power and Air Conditioning

The characteristics of the electrical and air conditioning systems permit compliance with the terms of use for all CA equipment, as defined by equipment suppliers.
Sites are equipped with both a primary electrical system and a backup system to ensure continuous and uninterrupted electricity supply. In addition, sites are equipped with primary and secondary ventilation or air conditioning systems to control temperature and relative humidity.

5.1.4 Exposure to water damage

Protection measures implemented by the CA protect its infrastructure against water damage.

5.1.5 Fire Prevention and Protection

The CA implements measures to prevent and fight fires.

5.1.6 Media Storage

All media used by the CA are processed and maintained in accordance with security requirements for confidentiality, integrity, and availability.
Measures have been implemented to protect media against damage, theft, unauthorized access, and obsolescence. These measures apply throughout the retention period for content stored on media. The media storage methods used to ensure that the CA's commitments regarding data recovery and long-term archiving are fulfilled.

5.1.7 Waste Disposal

At the end of its service life, media is either destroyed or reformatted for reuse, depending on the confidentiality level of data stored on it. Disposal procedures and methods comply with the Notarius Security Policy. Backups are regularly tested.

5.1.8 Off-site Backup

Adequate backups of the system and essential software applications are kept off-site to ensure that service may be restored following a system failure or disaster.
These backups are regularly tested and organized to provide the fastest possible disaster recovery.

5.1.9 Disaster Recovery

In addition to on-site backups, the C/RSP performs off-site backups of CCQ PKI applications and data. A disaster recovery plan is in place to ensure services are maintained and information remains available in the event of a failure of the primary system or of software essential to the delivery of CCQ PKI services following a disaster or storage media failure.

5.2 Procedural Controls

The following procedural security measures complement those described in the section on the Key

Ceremony held to create the CA Key Pair.
The security procedures and policies are communicated to employees.
Procedures are established and applied for all operations performed by personnel in trusted roles with the potential to impact on service delivery.
The CPS describes operational and administrative measures and controls to be implemented by the C/RSP to ensure that CCQ PKI operations remain secure.

5.2.1 Trusted Roles

The CCQ PKI administration includes trusted roles, ensuring a distribution of tasks such that there is no possible conflict of interest and no possibility of any person acting alone and circumventing the CCQ PKI security system.
The CA currently defines the following roles:

- ***Security Officer***: Responsible for the overall administration and implementation of security practises.
- ***Operations Manager/PKI Officer***: Responsible for certain operations performed on certificates. For example, the Operations Manager has access to the Security Manager and can perform digital signature registration, recovery, and revocation operations. It is the only person who can access the encrypted files of identity verification documents stored by the C/RSP.
- ***CCQ PKI Administrator***: Responsible for the administration and operation of CCQ PKI systems. The CCQ PKI Administrator oversees the set-up, configuration, and technical maintenance of an entity's IT equipment, in addition to the technical administration of an entity's systems and networks.
- ***Audit Log Auditor***: Authorized to perform monthly audits of CCQ PKI logs.
- ***Identity Verification Agent (IVA)***: Responsible for validating and confirming applicants' identities on behalf of the C/RSP.
- ***Affiliate Verification Agent (AVA)***: Responsible for validating and confirming, on behalf of the C/RSP, an applicant's professional association affiliation or employment relationship with a legal entity. The AVA confirms the validation result by approving or rejecting an application to issue a certificate.
- ***HSM Card Holder***: Responsible for keeping an HSM card required to operate the CA hardware security module.
- ***Authorized respondent of the CNQ***: Authorizes the notaries to use an official digital signature and may revoke this authorization according to the laws, regulations and contracts in force.

Any of the above-mentioned functional roles may be held by several individuals.
Procedures are established and applied for all administrative roles and trusted roles associated with the provision of certification services.
These roles are included in the c/RSP's employee job descriptions.
Appropriate access control mechanisms are also in place.
Background checks on individuals with trusted roles are reviewed in the C/RSP at planned intervals.

5.2.2 Number of Persons Required per Task

The number of persons required to be present as stakeholders or witnesses for each task is stipulated

in either the CPS or the C/RSP's internal procedures. This number is determined based on the type of operation performed, the number of persons required and their position.

5.2.3 Identification and Authentication for Each Role

The CA verifies the identity and permissions of all members of its personnel before assigning them roles and corresponding rights, either upon taking office or when new responsibilities are assigned for trusted roles, including:

- Adding the personnel member's name to access control lists for facilities housing the systems involved in their role;
- Adding personnel members' names to the list of persons authorized to physically access said systems;
- Opening a user account on behalf of the personnel member in said systems;
- Issuing cryptographic keys and/or certificates to perform a role assigned under the CCQ PKI.

These controls are described in the CA's CPS and comply with the Notarius Security Policy.

5.2.4 Roles Requiring Separation of Duties

Multiple roles may be assigned to the same individual provided that this multiplication of roles in no way compromises the security of the services provided, and that any associated risk has been agreed to by the CA's Information Security Manager (ISM).
A trusted role may also entail access to secret information.
A person cannot combine several trusted roles whose secrets are, or appear to be, irreconcilable with each other.

5.2.5 Risk Analysis

Notarius performs a risk analysis to identify threats to the CCQ PKI. This analysis is reviewed at least once per year, or during significant structural changes.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All individuals working at the C/RSP are subject to strict confidentiality and information security requirements. The Human Resources Manager is responsible for ensuring that duties assigned to all personnel working within the CCQ PKI corresponds to their professional skills. All supervisory personnel must possess expertise appropriate to their roles and be familiar with the security procedures and privacy protection measures in force.

5.3.2 Background Check Procedures

Before appointing an individual to a trusted role, a criminal background check is performed.

The CPS describes the procedures used to identify and authenticate personnel appointed to trusted roles. Personnel in trusted roles must be free from conflicts of interest that might jeopardize the impartiality of their duties.

5.3.3 Training Requirements

All individuals holding positions related to the provision of CCQ PKI services have received appropriate training to perform their duties. Areas in which they have been trained to include software, hardware, and all internal operating and security procedures that they are responsible for implementing and adhering. People in trusted roles know and understand the implications of the operations they are responsible for performing.

5.3.4 Retraining Frequency and Requirements

Individuals in trusted roles are informed or receive training about any changes made to systems, procedures, or organizations that affect their work.
All such individuals are also trained in incident management and in reporting and escalation procedures.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Disciplinary procedures are in place and appropriate sanctions are applied whenever an employee fails to comply with applicable security procedures and policies or the provisions of the CP or CPS.

5.3.7 Independent Contractor Requirements

Requirements for independent contractors are set out in written agreements.
Independent contractors providing services at Notarius's facilities and/or at disaster recovery sites are also bound by the provisions of Section 5.3 of this document.

5.3.8 Documentation Provided to Personnel

The CP, CPS, and all procedures and processes arising therefrom, as well as all other relevant documents (user manual, etc.) are made available to all personnel in positions involved in the provision of CCQ PKI services. Specifically, security rules are communicated to personnel when they take office, depending on the role assigned.

5.4 Audit Log Procedure

Event logging consists of manually or electronically recording a log of events, either by data entry or automatic generation. The resulting logs must permit traceability and accountability of the operations performed.

5.4.1 Types of Events Recorded

Several types of events are recorded.

Essentially, all events related to CCQ PKI security and services are recorded; all security and audit logs are retained and made available during compliance audits; and all events related to the life cycle of certificates are recorded to maintain traceability of actions performed by individuals in trusted roles.

Such events include, but are not limited to:

- Automatically recorded events:
  - Creation/modification/deletion of corresponding authentication data;
  - Start-up and shutdown of computer systems and applications;
  - Log-related events;
  - Successful and unsuccessful login and logout attempts made by users in trusted roles;
  - Unexpected shutdowns or detection of system hardware errors;
  - Router and firewall activity.

- Events requiring manual entries:
  - Physical access;
  - System maintenance and/or configuration;
  - Destruction of media.
- Function-specific events:
  - Receipt, approval or rejection of certificate applications;
  - Events related to signing keys and CA certificates;
  - Publication and updating of information related to the CA;
  - Generation of subscriber keys and certificates;
  - Processing of revocation requests;
  - Generation and publication of CRLs.

Accountability for a given action resides with the person, organization, or system that executed it.
The operator's name or identifier is explicitly recorded in the appropriate event log field.
Logs are updated as events happen.
Manual log entries are made on the same workday as the event, with some exceptions.

5.4.2 Frequency of Processing Log

Audit logs are periodically reviewed. In addition, automated reviews are performed on audit logs to identify abnormal activities and alert personnel of potential critical security events.

5.4.3 Retention Period for Audit Logs

Audit logs must be retained for an appropriate period in order to provide, where appropriate, the necessary legal proof as required by applicable legislation.

5.4.4 Protection of Audit Logs

Audit logs are always protected in such a way as to prevent alterations and ensure their confidentiality, integrity, and availability. Audit logs are recorded using techniques to ensure they cannot be deleted or destroyed for the duration of the audit logs retention period.

5.4.5 Audit Log Backup Procedure

Specific persons with specific access rights identified in the C/RSP can access event logs.

See the CPS for details.

5.4.6 Notification of recorded events sent to the originating source

Not applicable

5.4.7 Vulnerability Assessments

Measures have been implemented to perform vulnerability assessments to reduce or eliminate threats to CCQ PKI assets.

5.5 Records Archival

5.5.1 Types of Records Archived

Archiving ensures the long-term survival of CCQ PKI logs. It also ensures that specific information about certification operations is retained and remains available if needed. At the very minimum, the following information must be archived:

- CP;
- CPS;
- Certificates, CRLs, and OCSP responses;
- Audit logs;
- Repository data;
- Installation media for operating systems, CCQ PKI applications, and the repository;
- Database used by the C/RSP's application to manage subscriber data;
- Client files.

5.5.2 Archive Retention Period

Archiving periods include the following:

- Information collected to establish subscribers' identity: At least 10 years after validation.
- Signing certificates and public keys, and encryption certificates and keys: At least 10 years after the revocation or expiration of subscribers' keys and certificates.
- Data backups: From 1 day to 10 years, depending on the data concerned.

Notarius maintains a detailed data retention schedule and implement procedures to ensure data are archived for the stipulated periods.

5.5.3 Protection of Archives

Archived records are saved in such a way that they cannot be deleted or destroyed during their retention period. Archive protection measures are in place to ensure that only authorized persons can access and manipulate the archives, and only without altering the integrity, confidentiality, or authenticity of the data. Archived records remain readable and usable throughout their entire life cycle.

Procedures governing data retention, destruction, and transfers are in place and detailed in the CPS.

5.5.4 Requirements for Timestamping of Records

Certificates are dated at the time of generation, and date information is archived with the corresponding certificate. Section 6.8 stipulates dating and time-stamping requirements.

5.5.5 Archive Collection System

The system collects archive information in accordance with the appropriate security level for privacy protection. The CPS specifies the means used to securely collect archive information.

5.5.6 Procedures for Obtaining and Verifying Archive Information

Archives must be recoverable within 24 hours. Archive recovery conditions are stipulated in the CPS.

5.6 Key Changeover

The CA may not generate a certificate whose end date is later than the expiration date of the corresponding CA certificate. For this reason, the validity period of the CA certificate is longer than that of the certificates it signs.

Regarding the CA certificate validity end date, its renewal will be requested within a period at least equal to the lifetime of the certificates signed by the corresponding private key.

As soon as a new CA key is generated, only the new private key may be used to sign certificates. The previous certificate may continue to be used to validate certificates issued under this key, at least until all the certificates signed with the corresponding private key have expired.

5.7 Compromised Keys and Disaster Recovery

5.7.1 Incident and Compromised Key Handling Procedures

The C/RSP uses escalation and incident handling procedures and measures in accordance with the requirements of the Notarius Security Policy. These measures make it possible to minimize damage in the event of an incident.

5.7.2 Corrupted Computing Resources, Software and/or Data

In accordance with the Notarius Security Policy, a Business Continuity Plan is in place to meet the availability requirements for critical functions, including those arising specifically from this CP and other functions necessary to uphold commitments related to the publication and revocation of certificates. This plan is tested at least once every two (2) years.

5.7.3 Compromised Private Key Procedures for Entities

Cases of compromised CCQ PKI participants' private keys are handled in accordance with Section 5.7.2, "Corrupted Computing Resources, Software and/or Data."

Specifically, in the event of a compromised CA key, the Notarius C/RSP will do the following:

- Inform all impacted subscribers, as well as Relying Parties with whom the CA has signed agreements;
- Indicate that the certificates issued by the CA, as well as the published revocation status, are no longer valid;
- Immediately revoke all impacted certificates.

5.7.4 Business Continuity Capabilities after a Disaster

Business continuity capabilities after a disaster are addressed in the Notarius Business Continuity Plan (BCP). The BCP describes the steps to follow to resume CCQ PKI operations, in either a fully functional or a degraded mode, and for eventually resuming normal operations after being destroyed or damaged resources have been repaired or replaced.

5.8 Termination of Activities

5.8.1 CA Termination

The CA shall notify the C/RSP and the LRA at least six (6) months in advance of its intention to cease operating as a Certification Authority.
The terms and conditions for the transfer of operations and responsibilities to a third party are decided between the CA and the C/RSP and are then communicated to the LRA.
Commitments are detailed in the CPS.

5.8.2 C/RSP Termination

The C/RSP must notify the CA and the LRA at least three (3) months in advance of its intention to cease operations. Transfer arrangements must be approved by the CA and are then communicated to the LRA.
The C/RSP will arrange for the transfer of files and data to another certification and repository service provider (C/RSP) designated by the CA.

5.8.3 LRA Termination

When possible, the LRA must notify the CA at least three (3) months in advance of its intention to cease operations.

5.8.4 End of Life of the Key Management Infrastructure

In the event that a CA key is compromised, the CA will immediately cease to operate, and all valid certificates issued by the CA will be revoked. In order to return to the required service level, a new CA must be created, and new certificates issued.

6 Technical Security Controls

The requirements described below are minimum requirements that the CA must adhere to.
Additional requirements will be added and developed into security measures stipulated in the CPS.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Keys

CA signing keys are generated under strictly controlled conditions, by personnel in trusted roles, through "key ceremonies."
Root CA key pairs are always generated in the presence of at least two persons in trusted roles, i.e., the Security Officer or Operations Manager.
The key ceremony is accompanied by a signed statement confirming it was conducted in accordance with the applicable procedure and certifying the integrity and confidentiality of the key pair.

6.1.1.2 Subscriber Keys Generated by the CA

Subscriber key generation is performed in a secure environment. Keys are generated in a cryptographic module that complies with all applicable laws, regulations, and standards.

6.1.1.3 Subscriber Keys Generated by Subscribers

Not applicable.

6.1.2 Private Key Delivery to Subscribers

Keys are generated on subscribers' workstations or on a cryptographic hardware device equipped with the C/RSP application.
Once delivered, the private key remains under the sole control of the subscriber.
The CA does not retain or copy private keys.

6.1.3 CA Public Key Delivery to Relying Parties

The CA's public signing key is made available to subscribers and Relying Parties and is publicly available for viewing. Each time the CA's public key is sent to and from the CA's servers, its integrity is protected, and its origin is authenticated.

6.1.4 Key Sizes

The key size of the root CAs is RSA-4096 bits.
The key size of the root CA certificate holders is RSA-2048 bits.

6.1.5 Generating Public Key Parameters and Quality Control

The parameters and signature algorithms implemented in crypto-boxes, hardware, and software are documented by the CA.
Key generation equipment uses parameters that comply with security standards specific to each key's algorithm.

6.1.6 Key Usage

The sole allowable use of the CA private key and associated certificate is for signing CA and CRL certificates.

The use of subscribers' private keys and associated certificates is strictly limited to the purpose of providing signatures.

6.2 Protection of Private Keys and Cryptographic Modules

6.2.1 Cryptographic Module Standards and Controls

Modules used for both key generation and cryptographic operations meet recognized industry standards. Specifically, the modules used for key generation and cryptographic operations comply with the FIPS-140-2 specifications recognized by the U.S. National Institute of Standards and Technology (NIST) and adopted by Canada's Communications Security Establishment (CSE). The FIPS-140 Publication Series sets out requirements and standards for software and hardware cryptographic modules. FIPS 140-2 ensure key protection with a security level deemed acceptable against threats to integrity, availability, and confidentiality.

6.2.2 Protection of the CA's Private Keys (and their control by multiple individuals)

The CA's private keys must be stored in a hardware device certified at or above FIPS 140-2 Level 3.

Two employees in appropriate trusted roles are required to conduct all operations on the CA's private key.

6.2.3 Private Key Escrow

Subscribers' private keys are not escrowed.

6.2.4 Private Key Backup

A backup copy of the private decryption key can be retained by the Issuing CA in anticipation of a future recovery, provided that appropriate security measures are in place to preserve its integrity.

6.2.5 Private Key Archiving

Subscribers' private keys may under no circumstances be archived by the CA or by any other CCQ PKI participant.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The subscriber's private key may be transferred to the cryptographic module in accordance with the requirements of section 6.1.1.2.

6.2.7 Private Key Storage in the Cryptographic Module

Subscribers' private keys are protected by their cryptographic modules.

6.2.8 Multi-user Control (m of n)

The CA's private signing keys are controlled by no fewer than two (2) individuals in trusted roles in

accordance with the "m of n" authentication method.

6.2.9 Protecting Subscribers' Private Keys

Subscribers are solely responsible for the protection of their private keys.
This includes taking all necessary measures to ensure the security and confidentiality of their private keys, in particular by choosing a password that meets specific criteria stipulated by the C/RSP.

6.2.10 Private Key Activation Method

6.2.10.1 Activating the CA's Private Key

The CA's private key may be activated only by an authorized person, and only in the presence of at least two people.

6.2.10.2 Activating the Subscriber's Private Key

The subscriber's private key activation is controlled through the use of activation data.
Additional details can be found in the CPS.

6.2.11 Private Key Deactivation Method

6.2.11.1 Deactivating the CA's Private Key

This issue is addressed in other documents specific to the CCQ PKI. Deactivation modes are specific to the module technology used; details can be found in the manufacturer's documentation.

6.2.11.2 Deactivating the Subscriber's Private Key

Not applicable.

6.2.12 Private Key Destruction Method

6.2.12.1 Destroying the CA's Private Key

At the end of the CA private key's life, whether on its anticipated expiration date or prior to it (if it is revoked), the key is automatically destroyed along with any and all copies or items permitting its reconstruction.

6.2.12.2 Destroying the Subscriber's Private Key

Subscribers' private keys must be automatically destroyed upon the expiration of any associated certificates. The key is then automatically destroyed along with any and all copies or items permitting their reconstruction.

6.2.13 Evaluation of the Cryptographic Module

The cryptographic module responds to FIPS 140-2 Level 3.

In particular, it meets the following security requirements (non-exhaustive list):

- Ensures the confidentiality and integrity of the CA's private signing keys throughout their lifetime, including destruction according to high security standards;
- Identifies and authenticates its users;

- Creates audit records.

6.3 Other Aspects of Key and Certificate Management

6.3.1 Public Key Archival

CA and subscriber public keys are archived as part of the archiving process for their corresponding certificates.

6.3.2 Certificate and Key Usage Periods

In principle, the operational life of a certificate ends either when it expires or is revoked.
CA servers cannot issue certificates with a lifespan that exceeds the CA's own certificate.
Key usage periods are as specified in the CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data used to issue the Root CA or an Issuing CA's certificate, and associated with its storage in a hardware module, requires a key ceremony.
Subscriber activation data only becomes accessible once subscribers have identified themselves to the C/RSP, by means that include authenticating their identity on the Notarius website and answering security questions set during registration for a product/certificate type. Activation data delivery is thus kept separate in both time and space from private key delivery.

6.4.2 Activation Data Protection

The integrity and confidentiality of activation data generated by the CA for CCQ PKI cryptographic modules are protected until the activation data is delivered to the recipient. After delivery, the recipient is responsible for ensuring the confidentiality, integrity, and availability of said data.
The integrity and confidentiality of activation data generated by the CA for cryptographic partitions is protected until it is delivered to the recipient. After delivery, the recipient is responsible for ensuring the confidentiality, integrity, and availability of said data.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

The integrity and confidentiality of private keys or infrastructure and control secrets are protected in accordance with the Notarius Security Policy.
To achieve these security objectives, reliable systems and products are used to securely implement the various CCQ PKI processes. Systems and products are chosen or developed with security requirements in mind.
Computer security controls, defined in the CPS, meet the following security objectives:

- Identification and authentication of users for system access;

- Management of user sessions (logout after idle time, file access controlled by user role and username);
- Protection against computer viruses and all forms of compromising or unauthorized software and software updates;
- Management of user accounts, including the modification and removal of access rights;
- Protection of the network against intrusion, and to ensure the confidentiality and integrity of all data entering and leaving it;
- Audit functions.

6.6 Life Cycle Technical Controls

Control measures described in the CPS, including but not limited to the following, must be implemented to maintain the CCQ PKI's trust level:

- Documentation of all changes or evolution in the CCQ PKI;
- Saving of updates applied to the CCQ PKI;
- Auditing of the event logs;
- Auditing of the integrity and availability of the CCQ PKI.

To ensure the trust level is maintained, the C/RSP conducts a global risk analysis of the CCQ PKI components that support or are intended to support PKI services.

During installation, and periodically after installation, the C/RSP also tests the integrity of its systems.

6.7 Network Security Controls

The CA undertakes to ensure that all networks used as part of the CCQ PKI meet the IT security objectives set out in the CPS. Specifically, the CA must:

- Develop and update a network architecture diagram;
- Prohibit the connection of personal IT equipment to the network;
- Set up partitioned networks.

6.8 Timestamping and dating system

The dating systems are synchronized through a reliable universal time standard (UTC) and a Network Time Protocol (NTP) server that is precise to within one minute. All CA components, including CCQ PKI servers, are regularly synchronized using this time server. The information provided is used to reliably establish the date of the following:

- The beginning of a CA certificate's period of validity;
- The revocation time of a CA certificate;
- The publication of updates to the CRL;
- Logged events.

7 Certificate, CRL, OCSP, and TSA Profiles

7.1 Certificate Profile

The CA issues certificates in a format that complies with the specifications of X.509, version 3 described in RFC 5280 "Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile."
In each X.509 v3 certificate, the CA and the certificate holder are identified by an X.509 v3 Distinguished Name (DN).

Digital thumbprints are distinguished as follows:

PKI name	Fingerprint (thumbprint)
Centre de Certification du Québec (2010-2030)	2f 09 30 d1 b4 ab 87 cb e6 52 0b 10 60 94 3e 2d e8 4f 04 fb
Centre de Certification du Québec (1999-2019)	9e 81 30 7c f4 4c 09 9b 10 bf 41 da 8e dd d6 72 33 fb 58 fc

See SPC for details.

7.2 CRL Profile

CRLs comply with X.509, version 3.
cn=CRL1,ou=AC1,o=CENTRE DE CERTIFICATION DU QUEBEC,c=CA

See SPC for details.

7.3 OCSP Profile

Notarius offers the option to check the status of certificates through Online Certificate Status Protocol (OCSP) responders. OCSP responders can respond in real time to requests for the status of a particular certificate without having to download the CRL.
The Notarius OCSP supports the RFC 6960 standard.
OCSP responses contain validity dates that enable users to establish whether the OCSP response is sufficiently up to date for their intended use.

See details in the CPS.

7.4 TSA Profile

Not applicable.

8 Compliance Audit and Other Assessments

Audits and assessments include those performed as part of the qualified certificate delivery process, in the meaning of eIDAS, as well as those performed by the C/RSP to ensure that the entire CCQ PKI fully complies with this CP, the CPS, and all related security policies, all in order to ensure full compliance with all applicable security standards and legislation.

8.1 Frequency and/or Circumstances of Assessments

Before any major PKI participant begins service, or after any CCQ PKI component undergoes a significant change, the C/RSP must conduct a compliance audit of said component.

As part of the C/RSP audit program, internal and external certification and/or verification audits are conducted annually to obtain and maintain eIDAS accreditations [ETSI EN 319 401, ETSI EN 319 411-1 & ETSI EN 319 411-2], as well as ISO 27001 and ISO 9001 certifications.

8.2 Identity/Qualification of Assessor

Audits and assessments will be performed by assessors with expertise in system security or the specific area of activity of the PKI participant under assessment.

Designated auditors may be internal (C/RSP personnel) or external (contractors).

Internal auditors who are unable to perform the audit due to lack of knowledge must contract the services of a competent external auditor until they have completed appropriate training to obtain the required knowledge level.

Auditors must uphold stringent standards to ensure all policies, statements, and services are properly implemented and detect any nonconformity that could compromise the security of the services provided.

8.3 Assessor's Relationships to Assessed Entity

Internal auditors are appointed by the C/RSP, which authorizes them to monitor the practices of the target component of the audit.

External auditors are appointed by the C/RSP and must be independent and free of any conflict of interest with the CA and the C/RSP.

8.4 Topics Covered by the Assessment

Auditors perform compliance verification and controls of the certification services based on the CP, CPS, and related processes.

For external audits, the scope of topics or elements to be audited may be narrower or more specific. The auditor will establish an audit program that precisely defines which certification service participants are to be audited.

8.5 Actions Taken as a Result of Deficiency

Following an external audit, the external auditor must submit a formal and confidential report to the C/RSP outlining specific deficiencies and improvement opportunities. It is then up to the C/RSP to propose a timetable for resolving deficiencies and measures to be implemented.

In all other circumstances, deficiencies may be reported to managers who will then take the appropriate actions, if necessary.

8.6 Communication of Results

The results of the compliance audits are made available to the certification body responsible for CA qualification.

9 Other Business-Related and Legal Matters

9.1 Fees

9.1.1 Subscription or usage Fees

Fees may be charged for the subscription to or use of a CCQ PKI product.
These fees will be billed according to the fee schedule published by Notarius on its Web site, or negotiated as part of a specific agreement.

9.1.2 CRL Access Fees and Certificate Status

When the volume of verifications is substantial, or the verification service requires a specific level of service, fees may be charged to Relying Parties who need to access the CRL to verify the validity of subscribers' certificates.
For this purpose, an agreement must be made with the C/RSP.

9.1.3 Identity Verification Fees

- Identity checks performed by the C/RSP IVA may be invoiced to the Buyer.
- Additional discretionary fees may apply for identity verifications carried out by notaries, authorized guarantors for the verification of the identity of members in good standing of their professional Order. The fees charged are at the discretion of the authorized guarantors and the C/RSP has no control over them.

9.1.4 Fees for Other Services

Other services may be charged. In such cases, all persons affected by said fees will be notified.

9.1.5 Refund Policy

In compliance with the general terms and conditions of use, Notarius will only reimburse the Buyer the Subscription Fees that meet the following requirements: (i) in the event that an LRA or an employer refuses an application for Subscription to one or more Products; or (ii) if the Holder is unable to install the applications required to activate his Digital Signature.
All other fees and payments are non-refundable, non-cancellable and non-creditable during the Subscription period, including in particular in the event that the Holder is no longer a member of the RPA.

9.2 Financial Responsibility

The CP sets no limitations on the value of transactions for which certificates may be used. However, the contract of use may limit the type and value of transactions that can be made with the certificate.

9.2.1 Insurance Coverage

Risks liable to incur liability on the part of Notarius are covered by appropriate insurance. Any specific contractual agreement on insurance will take precedence over Notarius' usual general commitments in this matter.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for User Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The C/RSP's Privacy Policy, available on its website, describes the procedures used to process all information it collects, uses, discloses, and retains.
The following information held by the C/RSP is considered confidential (non-exhaustive list):

- Certain personal information related to the subscriber that is not contained in certificates;
- Private keys and information required for certificate management or recovery;
- CCQ PKI audit logs;
- Root CA and subordinate CA event logs;
- Audit reports;
- Client registration files;
- Records from the identity verification process performed by the IVA of the C/RSP;
- Causes for certificate revocation, unless their publication has been expressly authorized;
- Technical information relating to the operational security of certain components of the CCQ PKI and its infrastructure.

9.3.2 Information Not Within the Scope of Confidential Information

Information contained in certificates and CRL content is not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

Any and all collection of personal information by the CA must strictly adhere to all applicable regulations and legislation.

9.4 Protection of Personal Information

9.4.1 Privacy Plan

All information collected, used, retained, or disclosed in the provision of certification services is subject to the *Act respecting the Protection of Personal Information in the Private Sector* (R.S.Q., chapter P-39.1).
All information collected in connection with the issuance, use, or management of certificates must be used or disclosed solely for the purposes for which they were collected.
The C/RSP has implemented and maintains a privacy policy that is accessible to all and complies with applicable laws.

9.4.2 Information Deemed Private

Personal information is information that makes it possible to identify an individual or that is about an individual. Data from registration files not published in certificates or CRLs is considered confidential.

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Any and all collection of personal information by the CA must strictly adhere to all applicable regulations and legislation.

9.4.5 Notice and Consent to Use Private Information

Personal information transmitted to Notarius must not be disclosed or transferred to a third party, except under the following circumstances: prior consent of the person concerned, court ruling, or other legal authorization.
In this area, the CA complies with the Notarius Privacy Policy.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Records may be submitted as required to serve as evidence of certification in court, in accordance with the Notarius Privacy Policy.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Solutions Notarius Inc. ("Notarius") holds all intellectual property rights over the CP, CPS, and CCQPKI applications and technological infrastructure, including the CCQ PKI root certificate, the revocation information it issues & the name of this infrastructure, the Centre de Certification du Québec.

Subscribers hold all intellectual property rights to their personal data appearing on their certificates issued under the CCQ PKI. However, the subscriber acquires only the right to use the certificate and not ownership of the certificate itself.

Applications used to support the provision of certification services, or those used by subscribers, are and remain the property of their respective manufacturers. These manufacturers confer a licence to use the applications only, upon payment of associated fees.

The terms Notarius® and CertifiO® are registered trademarks of Notarius Solutions Inc.
Any reproduction or use of these trademarks without prior written authorization from Solutions Notarius Inc. is prohibited.

9.6 Representation and Warranties

9.6.1 Regarding Information Contained in Certificates

Mandatory information contained in certificates requiring a subscription must accurately reflect authenticated information, depending on the type of certificate requested.

9.6.2 Regarding Information in the Repository

The accuracy of CRLs published in the directory must be ensured.

9.7 Disclaimers of Warranties

Unless otherwise stipulated in a specific contractual agreement, the disclaimer of warranties is stipulated in the general conditions of use of Notarius products.

9.8 Limitations of Liability

Unless otherwise stipulated in a specific contractual agreement, the limitations of liability are described in the general conditions of use of Notarius products available on its website.

9.9 Indemnities

Unless otherwise stipulated in a specific contractual agreement, the cases of Indemnification are expressed in the general conditions of use of Notarius' products.

9.10 Approval Procedures

9.10.1 CP Approval Procedure

When the CP is amended, it must be submitted to the CA Board of Directors for approval.
Once these changes have been approved, the CP will be published on the CA website as soon as possible.
It may also be forwarded to LRAs in the event of significant changes that negatively affect their operations

9.10.2 CPS Approval Procedure

The CPS must comply with all approved changes to the CP.
When amendments are made to the CPS, they must be approved by the Board of Directors of the C/RSP.
Once the amendments are approved, the CPS will be published on the CHP/R website as soon as possible. The CA will also be notified.

9.10.3 Term of validity

This CP remains valid until replaced by a newer version, or until the CA ceases operations.
The end of validity of the CP also terminates all clauses that compose it.
Except for exceptional events directly related to security, the new versions of the CP do not require the revocation of certificates already issued.

9.11 Individual notices and communications with participants

In case of major changes to the PKIs components, the C/RSP's CISO will analyze the impact of such changes in terms of the security and quality of the services offered.

9.12 Amendments

The C/RSP ensures that all changes made to the PC remain in compliance with the laws, regulations and certification requirements.
Any major change to this CP could lead under certain conditions to a change in the OID number. Minor changes to the CP do not lead to a change of OID.
All new versions of the CP will be available on the CA's website.

However, in the case of changes having a major impact, personalized email notices will be sent, within a reasonable amount of time to be determined depending on the estimated negative impact of the change before the CP update. The informed persons must provide their comments with supporting evidence within the amount time which will be identified in the transmitted email. After this time, the changes will be implemented.
Major changes will be detailed on the CA's website in addition to the release of the new version of the CP.

9.13 Dispute Resolution Provisions

Certificates issued under this CP are bound by the terms of use set out in this CP and by the general terms of use of Notarius' products governing the relationship between Notarius and holders.

9.14 Governing Law

The resolution of disputes are detailed in the general conditions of use of Notarius' products.
Any dispute arising from the CCQ PKI services shall be resolved primarily through good faith negotiations.
If the conflict is not resolved through good faith negotiations within fifteen (15) days, it will then be submitted to mediation under the supervision of the Canadian Commercial Arbitration Centre and in accordance with its Conciliation and Mediation Rules in effect at the time of such mediation. If the dispute is still not settled within thirty (30) days following the notice of willingness to mediate, it shall then be finally settled under the aegis of the Canadian Commercial Arbitration Centre, by arbitration to the exclusion of the courts of law, in accordance with its General Commercial Arbitration Rules in effect at the time of such mediation. The arbitration shall be conducted by a single arbitrator sitting in Montreal.
The application of the UN Convention on Contracts for the International Sale of Goods is expressly excluded.

9.15 Interpretation

9.15.1 Applicable Laws

This CP is governed by and construed in accordance with the applicable laws of the Province of Quebec, and the federal laws of Canada applicable therein, without giving effect to any conflict of law's provisions.

9.15.2 Validity of Provisions

The fact that one or more provisions of the CP may be declared invalid, illegal, or unenforceable in no way affects the validity of the other provisions.
This CP, minus the unenforceable provision, will therefore continue to apply.

9.16 Force majeure

Force majeure is an external, unforeseeable, irresistible and uncontrollable event that makes it impossible to fulfil an obligation.
Are considered as cases of force majeure all those habitually retained by the Canadian courts and more specifically those resulting from the definition which is given of this expression in Section 1470 of the Civil Code of Quebec.

9.17 Review

The CCQ PKI CP is annually reviewed.

9.18 Effective Date

This CP comes into force on the date of its adoption by the Notarius Board of Directors.