Public release

NOTARIUS® PUBLIC KEY INFRASTRUCTURE

CERTIFICATE POLICY FOR THE ISSUANCE OF CLOUD DIGITAL SIGNATURES

Version: 1.0
OID 2.16.124.113550.2
Approval date: 2020-04-30

Notes

A new product is now available in ICA1, the Cloud Digital Signature.

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
1.0	2020-04-30	First version of the rules governing the issuance of Digital Signatures Cloud of tests & for employees	Maud Soulard, PKI Officer	Board of Solutions Notarius Inc.

Intellectual Property

Table of Contents

1 General Provisions

1.1 Overview

As a trusted service provider, Solutions Notarius Inc. (hereinafter "Notarius") has for many years had the mission of offering digital signature solutions that ensure the long-term reliability of documents.
At the same time, Notarius has also developed the electronic signature market.

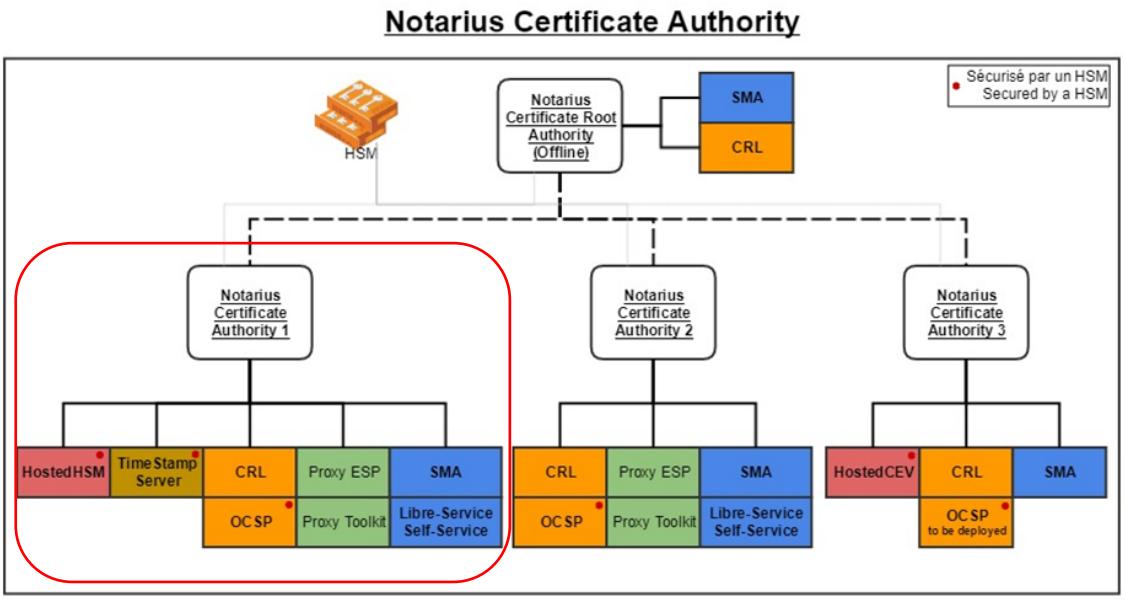
Being at the forefront of technology, attentive to the needs of its stakeholders and taking into account the evolution of technology, the ever-increasing importance of cloud computing and mobile equipment in particular, Notarius had to enhance its product offering.
Notarius' new Cloud Digital Signature solution will enable holders to digitally sign documents without having to install elements of the signature (e.g. private key) locally on their workstations.

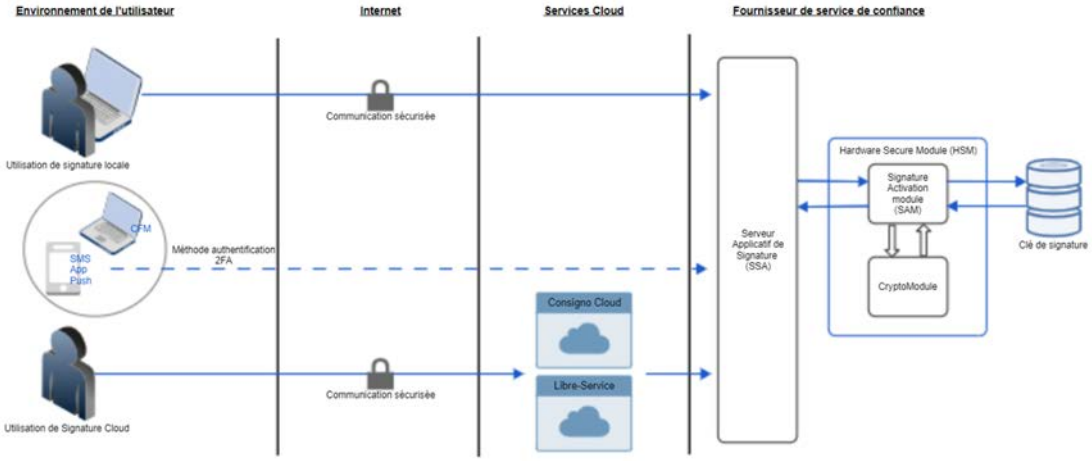
Indeed, for Cloud digital signature creation, the signature creation data will be stored and managed by a trusted third party (Notarius) on behalf of the holder. To ensure that the signature creation environment is reliable and that the signature creation data is used under the control of the holder, Notarius must apply strict administrative security procedures and use reliable systems and products, including its communication channels.

This Certificate Policy (hereinafter the "CP") therefore defines Notarius' commitments in the context of providing Cloud Digital Signatures.
To set up the architecture of this new service, the Notarius team referred to the technical specifications of ETSI TS 119 431-1.
It was also inspired by ILNAS-EN 419241-1:2018 for the SSA (Server Signing Application) portion & ILNAS-EN 419241-2:2019 for the SAM (Signature Activation Module) portion.

As the Main Infrastructure remains that of iCA1, the CP still complies with the general principles and recommendations defined in ETSI EN 319 401, ETSI EN 319 411-1&ETSI EN 319 411-2.

As Notarius is the holder of several PKIs, the scope of this CP is limited to iCA1 only.
The version of this CP is limited to Test Cloud and Employee Cloud Digital Signature products only.





1.2 Document Identification and Object Identifier Numbers (OID)

This CP is called the *Notarius Public Key Infrastructure Certificate Policy*. It is identified in particular by its object identifier number (OID) as follow: 2.16.124.113550.2

The CP is supplemented by a corresponding *Certification Practice Statement* (CPS), also referenced by an OID number: 2.16.124.113550.2
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 Notarius PKI consist of the following:

- (2) country
- (16) Canada
- (124) Notarius
- (113550.2) Notarius Authority
- …

Cloud certificates generated and managed by Notarius on behalf of the holder have the following OID number: 2.16.124.113550.2.2.4.3

1.3 Definitions and Abbreviations

1.3.1 Abbreviations

The abbreviations used in the CP are as follows:

- **AATL**: Adobe Approved Trust List
- **CA**: Certification Authority
- **CISO**: Chief Information Security Officer
- **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
- **FIPS :** *Federal Information Processing Standard*
- **HSM**: Hardware Security Module
- **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
- **RPO**: Recovery point objective
- **RTO**: Recovery time objective
- **SAM:** Signature Activation Module
- **SLA:** Service Legal Agreement
- **SSA:** Server Signing Application
- **SS**: Self-Service

1.3.2 Definitions

The terms used in this CP have the following meanings:

- **Activation**: Operation performed by the holder that consists of entering an activation number and a personalized code in a cryptographic device (HSM) to generate its certificates, thus activating its Cloud Digital Signature.
- **Activation data**: Information needed to activate keys and certificates that the subscriber must protect to ensure confidentiality (e.g., a password and a punctual code transmitted via a 2nd channel).
- **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) in order to grant the subscriber access to resources (systems, networks, or applications).
- **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. This set of information attests that a key pair belongs to a natural person identified in the certificate. The certificate is valid for a specific period that is specified in the certificate.
- **Certification Authority (CA)**: Entity responsible for certificates signed in its name as well as the PKI. 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 used by the holder, installed on a workstation or accessible online, that allows the holder to activate or retrieve their certificates, change their password, perform certain configuration operations or carry out transactions using their certificates. This client application may be referred to as the CSP/R Portal in this CP.
- **Cloud Digital Signature:** the private and public keys contained in a certificate hosted in the Cloud 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 Cloud Digital Signature certificate protected by authentication via an account with a username (email) and password followed by a second factor (code) transmitted via a second communication channel, which is securely delivered to a validated user. Cloud Digital Signatures issued by Notarius can be affixed to PDF, PDF/A, and any other type of supported documents. The types of Cloud Digital Signatures vary according to the Product(s) to which the user has subscribed. A Cloud Digital Signature remains valid until it expires or is revoked.
- **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.
- **Hardware Security Module (HSM)**: Hardware cryptographic device in which certification authorities' public and private keys are stored.
- **Holder:** A natural person that has subscribed to the service (by itself or by a purchaser) and that holds PKI keys and certificates enabling it to sign or authenticate 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.
- **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 PKI. A Relying Party may also be a PKI 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.
- **Signature Activation Module (SAM):** the SAM is a module deployed inside the HSM. Intra-HSM deployment allows to inherit security aspects of the HSM such as roles, permissions, audit logs, cryptographic functions, etc. The SAM used here was developed using the Utimaco SDK. The SAM performs the final authorization when using a private key.
- **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 undertakings and commitments as a supplier of qualified and advanced certificates, in accordance with ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.
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 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 or amend the CP;
- Choose 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 PKI, including the PKI Officers;

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

- Oversee the administrative and technological aspects of certificate issuance, such as validating the the identity and quality of certificate holders or the secure storage of documents;
- Perform subsequent operations pertaining to the certificate life cycle;
- Provide repository services to confirm the validity of certificates in accordance with CA requirements;
- 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.

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 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 that it has expressly identified to the C/RSP.

The LRA must:

- Always have at least one person to act as an Affiliation Verification Agent (AVA), and take all actions necessary to comply with this requirement;
- Ensure the management of AVA appointment;
- For each business day, ensure that the 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;

The LRA or its AVA must:

- Apply and comply with the CP;

- Approve or reject the registration of initial certificate applications submitted to it by confirming the applicant is employed by the LRA;
- 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 Subscriber

1.6.4.1 Definition

A PKI key or certificate subscriber is a natural person that uses its certificate to sign 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 stipulated by the C/RSP;
- Provide all information and documentation required by the C/RSP;
- Protect the confidentiality of their activation data, authentication data, and password;
- Ensure that he is the only one to use its certificates (exclusive control of the holder) or, when they are for testing purposes, to ensure that they are only used by authorized persons;
- Use their certificates for the authorized purposes only;
- Sign documents online to ensure their authenticity;
- Use all computer equipment (computer, tablet, cell phone or other) in a secure manner;
- Notify the C/RSP customer service as soon as possible if the Holder suspects that the confidentiality of his/her certificate, or its password(s), is compromised;
- Notify the C/RSP as soon as possible of any changes, through the Client Application "My Account";
- Stop using his/her certificate when it is revoked or has 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 a written agreement to this effect with the C/RSP.

The Business Partner must:

- Align its business processes with the use of Notarius PKI keys and certificates (hereinafter the "PKI");
- Comply with all technical and functional requirements stipulated by the C/RSP;

- Designate a person within their organization to hold PKI certificates;
- Manage user access and permission for its IT applications;
- Ensure that all necessary updates reflect changes to the PKI;
- Inform subscribers of authorized uses of its applications;
- Ensure that holders are equipped to comply with all obligations arising from the Policy;
- Notify the C/RSP of any event that may require action to be taken on 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 PKI.
A third-party user may or may not be a PKI certificate subscriber/holder.
Any third-party user wishing to act based on a certificate must ensure that the certificate:

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

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.

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.

Notarius commercializes its expertise under several product lines and solutions such as digital signatures, electronic signatures, certification and authentication solutions for electronic documents in particular. The table below specifies the Cloud Digital Signatures currently available in the CertifiO® range and provides a brief description of the appropriate uses of Notarius' products/type of certificates.
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 Employees	Cloud 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. Also certifies the employer's name.
CertifiO for Evaluation	Cloud Digital signature certificate for testing purposes only; may not be used in a different context. Does not certify the identity, professional status or relation to the employer. The certificate includes metadata which indicates to Adobe Acrobat and ConsignO that the identity of the signatory has not been verified and is therefore not reliable.

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, agreements on the level of service or specifications of a product may limit the uses that the holder of its certificates may make, including the number of uses.
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.

In addition, subscribers undertake not to use certificates that have been revoked or expired.

Finally, any use not specified in this CP is strictly prohibited.

Notarius cannot, under any circumstances, be held responsible for the use of the certificates issued under this CP for purposes and under terms other than those expressly provided for herein.

1.7.3 Authorized Holder

The authorized holder is:

- An individual acting for a Legal Person (employee, agent, etc.) who wishes to use 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.

1.8 Policy Administration

1.8.1 Organization Administering the Document

This CP is under the responsibility of Notarius.

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 Notarius Board of Directors (hereinafter the "Board") is responsible for approving this CP on behalf of Notarius.
Notarius 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 provides users with information on the revocation status of valid certificates issued by the CA.
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)
- The General and specific Terms of Use for products offered by Notarius (https://notarius.com/en/legal-info/)
- Service Level Agreements (SLAs) 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: *Notarius Root Certificate Authority*
- The certificates of the issuing CAs are the Notarius Certificate Authority, increased by one digit if necessary;
- Valid and up-to-date CRLs:
    - http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl
- ARLs:
    - http://crl.notarius.com/notarius_root_ca/crl/crl_roota1.crl

2.3 Time and Frequency of Publication

Information related to the Notarius 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 is published on the Notarius website as soon as possible after its adoption by the CA. It is therefore available 24 hours a day, 7 days a week;
- The CPS is published on the Notarius website as soon as possible after its adoption by the Notarius Executive Committee. It is 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 (par.2.2) 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 PKI through strong controls (based on at least two-factor authentication) and an encrypted communication channel to ensure confidentiality.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

To identify a Cloud Digital 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 is presented in one of the forms below, depending on the product the user has subscribed to.

Product	UID (*Unique ID*)	CN (*Common Name*)	OU = (*fields certified by CRM*)	O = (*product name*)	C= (*name of the country*)
CertifiO for Evaluation	*Random identifier*	Test - *Contact first and last name - -Account name* *(Warning, **if** evaluation products, then will necessarily be Notarius Evaluation)*	*Name in the DN of the account* **or** *Account name*	CertifiO Test - Cloud	C=CA
CertifiO for Employees	*Professional email address*	*Contact first and last name -- Short name of the account or Name in the DN of the account or Name of the account*		CertifiO - Empl. - Cloud	C=CA

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 depend on the type of certificates issued.

3.1.5 Uniqueness of Names

Notarius guarantees the uniqueness of the names.
The uniqueness of the DN is guaranteed using a unique serial number and a combination of additional 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

The right to use a name that is a trademark, service mark or other, belongs solely to the legitimate owner of that trademark or to its licensees or assignees. 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. Notarius will not be held liable for any unlawful use by clients and beneficiaries of trademarks, registered trademarks, distinctive or other signs, as well as domain names.

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 a legal person, are detailed in the CPS.

Verification can also be used to establish the identity and existence of a legal person, device, application, or group.

3.2.1 Initial Identity Verification

The initial identity verification is required:

- To establish the identity of a natural person;

The initial verification of the identity of a natural person requires the presentation of 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).

Identity-related information about the applicant that is included in the certificate must match the information presented as part of the identity verification and to that on the membership form.

All identity documents submitted must allow the AVI to differentiate between individuals, including homonyms, regardless of attributes.

A third party must also be able to identify the holder with a high level of confidence, even if there are minor differences between the legal name or the common name.

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) in the cases specified in the CPS, except for *CertifiO Test – Cloud* product.

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 steps of this process are also detailed in the CPS.

Once identity has been verified, confirmation of employment for employee signatures will be required. See below.

Note that prior validation of the legal existence of the organization is systematically performed each time an account is opened with the PSC/R.

3.2.1.1 Identity Verification (IV) by an Authorized Agent

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

- Standard: An authorized employee (IVA) of the C/RSP;
- Exception: An authorized employee of a legal entity that has signed a written agreement with the C/RSP.

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

However, in some cases, companies may request to forego this identity verification process (by the C/RSP's authorized IVA) and instead use their own internal process. In such cases, an IVA must be specifically assigned to the file.

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).

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

3.2.1.3 Affiliation Verification by an Authorized Entity

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

- Confirmation of the applicant's employment relationship by a legal person is deemed to mean they are authorized to hold 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 employment relationship.

3.2.1.4 Interoperability Criteria

The CA is not party to mutual recognition agreements with any CA outside its security domain.
The Notarius PKI is recognized by Microsoft's Capi.

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 a Re-key

When the holder requests the re-issuance of his Cloud Digital Signature within twelve (12) months of its revocation, expiration, or cancellation, he must successfully authenticate himself on the C/RSP Portal (via his account with username and password followed by a 2nd factor transmitted through a second communication channel).
Failing this, applicants will be required to have their identity revalidated in accordance with the procedure described in section 3.2.1.
Re-issues are not applicable for CertifiO for Organizations. A new issue is preferred.

3.2.4 Identity Validation for Certificate Modifications

When the holder wishes to change certain information contained in his certificate, he must successfully authenticate himself to the PSC/R portal [via his account with username (email) and password followed by a 2nd factor (code) transmitted via a second communication channel (e.g. mobile app, SMS, phone call, etc.)] in order to make the desired changes himself (the fields that can be changed are: phone number, country and province).

As any other changes are not allowed via the CHP/R portal, the holder will then have to apply to revoke his certificate and request a new one with the correct information. A new verification of identity will have to be performed if necessary.

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.
- Fill in the account creation information (the holder must document his personal information, the password chosen for his new account, his mobile phone number, his date of birth).
- Validate the new account via SMS.
- 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.

4.1.3 Approval or Rejection of Certificate Applications

Upon receipt of a request, once identity verification has been completed, manual validations are made (verification and consistency of the certifications or documents provided) by the PSC/R, who must accept or reject it. In all cases, the claimant is notified of the decision using the information provided by the claimant during the application process.

4.1.3.1 Approval or Rejection of a Cloud Corporate Digital Signature Application

Applications for Cloud 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 validity or 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 entity, or employment relationship via the restricted-access Notarius digital signature management platform.

4.1.3.2 Approval or Rejection of other Types of Cloud Digital Signature Applications

Subscription applications are processed manually by the C/RSP's AVA. This includes individual digital signatures.

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

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.
    - If the applicant has paid by credit card, a refund is credited.

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.

4.2 Certificate Renewal Requests

Renewal of the subscription linked to the holder's certificate is possible.
However, renewal of the certificate itself is not. A recovery is necessary under the conditions set out below.

4.2.1 Renewal notice

Subscription renewal notices are sent by email at scheduled times.
Traces of these notices are kept in the contact's file.
Notices mentioning the occurrence of possible technical problems may also be sent by e-mail to the holder requesting the recovery of the certificate, if applicable.

4.3 Certificate Recovery

Recovery consists of issuing new keys and new certificates while the existing private key held by Notarius is still valid but non-operational, for example due to the loss of the password linked to the private key or the destruction of the keys.

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 client application or LS Portal (with an online VI).

4.3.3.2 In-person Recovery

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

4.4 Certificate Modification Requests

The modification consists of making changes to the information contained in the certificate, provided that the existing private key held by Notarius is still valid and functional.
Changes to the certificate are not yet available. A new issue is therefore preferred. The holder will have to make a request to retrieve his certificate and enter the correct information in his new request..

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 holder fails to comply with the certificate's applicable terms and conditions.
- The client, LRA, or CA fails to fulfill their obligations under the CP;
- A major error (intentional or unintentional) is identified in the holder's account information;
- The private key is compromised;
- The holder or an authorized person requests the revocation of the certificate;

- 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;
- Termination of the contractual relationship between the CA and the LRA prior to the end of the validity of the certificates.

When any of the above-mentioned circumstances occurs and the CA or the C/RSP becomes aware of this, the certificate in question is revoked as soon as possible.
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, including the general or particular conditions of use of Notarius' products.

4.5.1.2 PKI Participant Certificates

Various circumstances may result in the revocation of a certificate held by a particular 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 Notarius PKI upon discovery that one or more participant procedures are non-compliant with the CPS;
- The cessation of activities of the participant's operating entities.

The occurrence of one of these circumstances must be, without delay, brought to the attention of the CA or the C/RSP who must immediately revoke the certificate.

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.

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 to the C/RSP.

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;

- 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 upon receipt within a maximum of 24 hours of receipt.
They cover the receipt of the authenticated revocation request until the revocation information is made available to users.
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 PKI Participant Certificates

The CPS specifies the procedures to be implemented in the event of the revocation of 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 contact 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 all 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

Notarius generates and manages private keys on behalf of the certificate holder on a FIPS 140-2 level 3 or higher device and operates the cryptographic device on the basis defined by ETSI 119 431-1. In this situation, the certificate will include OID 2.16.124.113550.2.2.4.3.

An escrow agreement has been signed by the CA in the event that the CA ceases operations.

5 Facility Management and Operational Controls

The Notarius PSC/R is committed to implementing and maintaining an appropriate security policy, a level of physical and logical security as well as control mechanisms and service levels required for the operating premises of the PKI components.
The PSC/R conducts an annual risk assessment to identify internal and external threats and evaluate the probability and potential impact of these threats on Notarius' data and processes.
The PSC/R maintains and evolves its overall security program for:

- Protect the confidentiality, integrity and availability of data and processes.
- Protect against anticipated threats or risks to the confidentiality, integrity and availability of data and processes.
- Protect against unauthorized or illegal access, use, disclosure, alteration or destruction of data and processes.
- Protect against accidental loss or destruction or damage to data and processes; and
- Comply with all other security requirements applicable to the CA under the law and industry best practices.

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 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 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 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 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.

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 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 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 PKI operations remain secure.

5.2.1 Trusted Roles

In order to ensure that one person acting alone cannot circumvent security measures, responsibilities are shared among several roles and individuals. This is accomplished by creating separate roles and accounts for the different components of the CA system, and each role has a limited capacity.
PKI administration includes trusted roles that provide this division of labour so that there is no potential conflict of interest and no one individual can act alone to circumvent the security of the PKI system. Additional trusted roles are also in place to enhance the security of the HSM for issuing cloud digital signatures.
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.
- ***PKI Administrator***: Responsible for the administration and operation of PKI systems. The 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 PKI logs (in reading only).
- ***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 access holder***: Responsible for holding the HSM access and management required to operate the CA hardware security module.

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 CA's employee job descriptions.
Appropriate access control mechanisms are also in place.
Background checks on individuals with trusted roles are reviewed 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 CA'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 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. Individuals with such access may only hold a single role.

5.2.5 Risk Analysis

Notarius performs a risk analysis to identify threats to its 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 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 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 to within the PKI participant in which they operate. 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 PKI services. Specifically, security rules are communicated to personnel when they take office, depending on the role assigned. Personnel in operational roles within the PKI are given the relevant procedure documentation. All documentation is kept up to date.

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 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 PKI assets.

5.5 Records Archival

5.5.1 Types of Records Archived

Archiving ensures the long-term survival of 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;
- The general terms of use;
- Certificates, CRLs, and OCSP responses;
- Audit logs;
- Repository data;
- Installation media for operating systems, PKI applications, and the repository;
- Database used by the C/RSP's application to manage subscriber data;
- Client files including the information collected to establish their identity..

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 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 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 must notify the C/RSP and the LRA at least six (6) months in advance of its intention to cease operating as a Certification Authority.

In the event of the total cessation of the CA's activities, the entity that has been designated in the escrow agreement will ensure the publication of the CRLs. The procedures for transferring operations and responsibilities, including the revocation of certificates already issued, for example, will be agreed upon between the CA and the C/RSP. Each party's specific commitments are detailed in the CPS.

5.8.2 C/RSP Termination

The C/RSP must notify the CA 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

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 PKI

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

The holders' private keys are generated by Notarius in an HSM set up exclusively for this purpose.

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 algorithm and key size of the root CAs and iCA1 is RSA-4096 bits.
The algorithm and key size of the root CA certificate holders and iCA1 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.
See Section 7 for certificate profile details.

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 private keys and certificates of the holder is strictly limited to the signature service.

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 Level 3 and EAL 4+ 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 are 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

Notarius generates and manages private keys on behalf of the certificate holder on a FIPS 140-2 level 3 or higher device and operates the cryptographic device on the basis defined by ETSI 119 431-1. In this situation, the certificate will include OID 2.16.124.113550.2.2.4.3..

6.2.4 Private Key Backup

The private key will be retained by appropriate enhanced security measures to preserve its integrity (e.g. storage in secure cryptographic devices).

6.2.5 Private Key Archiving

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

6.2.6 Private Key Generation into or from a Cryptographic Module

The generation of the private key to the cryptographic module is done in accordance with the requirements of section 6.1. 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

Holders are solely responsible for the protection of their certificate access information's (e.g. password).
Notarius is responsible for the protection of private keys.
This includes taking all necessary measures to ensure the security and confidentiality of their private keys, in particular by using an HSM and strict access rights (see diagram in section 1.1).

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 certificate holder must be authenticated with the cryptographic module before the private key can be activated. This activation is controlled via 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 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 is 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.
The carrier's private key is generated in a cryptographic module wherein activation data is created and distributed during the initialization and customization phases.

6.4.2 Activation Data Protection

The integrity and confidentiality of activation data generated by the CA for 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 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.

Surveillance devices are also installed, such as video surveillance.

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 PKI's trust level:

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

To ensure the trust level is maintained, the C/RSP conducts a global risk analysis of the 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.

Any significant change in a PKI component must be documented and receive prior approval from the CISO of the C/RSP.

6.7 Network Security Controls

The CA undertakes to ensure that all networks used as part of the 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 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 of iCA1 is distinguished as follows:

PKI name	Digital Thumbprint
Notarius Root Certificate Authority	1f 3f 14 86 b5 31 88 28 02 e8 7b 62 4d 42 02 95 a0 fc 72 1a
Notarius Certificate Authority	bb 05 7f 07 4c 92 da db 5e 49 52 43 e2 59 a0 3f e1 6b d6 87

7.2 CRL Profile

CRLs related to iCA1 comply with X.509, version 3.

- http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl
- http://crl.notarius.com/notarius_root_ca/crl/crl_roota1.crl

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

See details in the CPS.

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 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 PKI participant undergoes a significant change, the C/RSP must conduct a compliance audit of said PKI participant.

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 & ETSI EN 319 412-3], 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 before beginning 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, minor deficiencies and improvement opportunities. It is then up to the C/RSP to propose an appropriate 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 Fees

Fees may be charged for subscribing to a Notarius PKI product.
These fees are in fact those that the Buyer must pay annually or monthly, as the case may be, for the use by a Holder of one or more Notarius PKI products, in addition to membership fees and transaction fees.
These fees will be billed according to the fee schedule published by Notarius on its website or negotiated under a specific written contractual 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.

9.1.4 Fees for Other Services

Other services may be charged, including unreasonable product usage fees. 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 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.

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.

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;
- PKI audit logs;
- Root CA and subordinate CA event logs;
- Audit reports;
- Client registration files;
- Records from the identity verification process;
- Causes for certificate revocation, unless their publication has been expressly authorized;
- Technical information relating to the operational security of certain components of the 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 of Quebec and Canada.

9.4.5 Notice and Consent to Use Private Information

Personal information provided 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 PKI applications and technological infrastructure.
Subscribers hold all intellectual property rights to their personal data appearing on their certificates issued under the 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.
Any reproduction or representation (including publication and dissemination), in whole or in part, by any means whatsoever of the items mentioned in this CP is strictly prohibited, including but not limited to electronic, mechanical, optical, photocopying, and computer recording.

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, the disclaimer of warranties is stipulated in the general conditions of use of Notarius products available on its website.

9.8 Limitations of Liability

Unless otherwise stipulated, 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 of this publication.

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.
Should any dispute arise from the PKI services, an initial attempt must be made to resolve it 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 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.