



Public release

CERTIFICATION PRACTICES STATEMENT

NOTARIUS® PUBLIC KEY INFRASTRUCTURE

Version: 3.4
OID: 2.16.124.113550.2
Approval date: 2022-11-15

Notes

One change has been made to this version of the Notarius Public Key Infrastructure (PKI) Certification Practices Statement (CPS):

- Review of the Policy in accordance with the requirements of eIDAS

*Note that most of the **procedures referenced** are classified as "Internal" and others as "Confidential." They are therefore not, as a matter of principle, accessible to the public. However, the public may submit a written request to the person in charge designated in Section 1.8.2.*

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 CPS, the French version will prevail.

Version Tracking

Version	Date	Description	Editor/Collaborators	Approving
1.2	2015/05/26	Initial version	Liette Boulay, Director - Legal & Compliance	Board of Directors of Solutions Notarius Inc.
1.3	2017-02-17	Changes to comply with the eIDAS standard	Maud Soulard, PKI Officer	Board of Directors of Solutions Notarius Inc.
2.0	2017-12-14	Update following the eIDAS qualification audit	Maud Soulard, PKI Officer Alexandre Provost, IT Team Leader	Board of Directors of Solutions Notarius Inc.
3.0	2019-12-16	Update following the eIDAS qualification audit Precision of processes related to CertifiO for Organizations and CertifiO for Departments products Addition of ICA3 and VDS	Maud Soulard, PKI Officer	Board of Directors of Solutions Notarius Inc.
3.1	2019-12-19	Update following the eIDAS qualification audit in accordance with ETSI EN 319 411-2 Standard CCS-6.3.10-13	Maud Soulard, PKI Officer	Board of Directors of Solutions Notarius Inc.

3.2	2020-10-26	Confirmation of the verification and validation of the holder's email	Maud Soulard, PKI Officer	Board of Directors of Solutions Notarius Inc.
3.3	2021-11-24	Insertion of new digital fingerprint	Maud Soulard, PKI Officer	Board of Directors of Solutions Notarius Inc.
3.4	2022-11-15	Changes for eIDAS compliance	Maud Soulard, PKI Officer Alexandre Provost, Security Leader	Management Committee of Solutions Notarius Inc.

Intellectual Property

This Certification Practices Statement is the exclusive property of Solutions Notarius® Inc. Any reproduction, printing or transmission of this document is strictly prohibited. For any reproduction in whole or in part, obtain prior written permission from Solutions Notarius Inc.

© 2022 Solutions Notarius Inc.

Table of Contents

1	General Provisions	9
1.1	Overview	9
1.2	Document Identification and Object Identifier Numbers (OID)	10
1.3	Definitions and Abbreviations.....	12
1.3.1	Abbreviations.....	12
1.3.2	Definitions	13
1.4	Interpretation.....	17
1.5	Compliance with Applicable Standards.....	17
1.6	PKI Components.....	17
1.6.1	Certification Authority (CA)	17
1.6.2	Certificate and Repository Services Provider (C/RSP)	17
1.6.3	Local Registration Authority (LRA)	18
1.6.4	Subscriber	20
1.6.5	Other Participants.....	21
1.7	Use of Keys and Certificates.....	21
1.7.1	Authorized Use of Keys and Certificates.....	21
1.7.2	Limitations of Use	23
1.7.3	Authorized Holder	23
1.8	CPS Management	23
1.8.1	CPS Manager.....	23
1.8.2	Contact Person	23
1.8.3	CP and CPS Approval Procedures	24
2	Publication and Distribution of Information.....	25
2.1	Publication and Repository Responsibilities	25
2.2	Publication of Certification Information	25
2.3	Time and Frequency of Publication	25
2.4	Access Controls on Repositories.....	26
3	Identification and Authentication	27
3.1	Naming	27
3.1.1	Types of Names	27
3.1.2	Explicit Names.....	27
3.1.3	Anonymization or Use of Pseudonyms.....	29
3.1.4	Rules for Interpreting Various Name Forms	29
3.1.5	Uniqueness of Names	29
3.1.6	Identification, Authentication and Role of Trademarks	29
3.2	Identity Validation	29
3.2.1	Initial Identity Verification	30
3.2.2	Identity Validation for Delivery of Activation Data	34
3.2.3	Identity Validation for Certificate Renewals.....	34
3.2.4	Identity Validation for a Re-key.....	35
3.2.5	Identity Validation for Certificate Modifications	35
4	Key and Certificate Management.....	36
4.1	Key and Certificate Issuance Request.....	36
4.1.1	Authorized persons.....	36
4.1.2	Application Process.....	36
4.1.3	Approval or Rejection of Certificate Applications	36
4.1.4	Term of validity of the request.....	39
4.1.5	Certificate Approval	39
4.2	Certificate Renewal Requests	39

4.2.1	Authorized persons	40
4.2.2	Certificate Renewal Procedure	40
4.2.3	Processing Certificate Renewal Requests	40
4.2.4	Renewal Notice	40
4.3	Certificate Recovery	40
4.3.1	Authorized persons	41
4.3.2	Procedure for Certificate Recovery.....	41
4.3.3	Processing a Certificate Recovery.....	41
4.4	Certificate Modification Requests	41
4.4.1	Authorized persons	41
4.4.2	Circumstances for a Modification	42
4.4.3	Processing Certificate Modification Requests.....	42
4.4.4	Notification of Modifications.....	42
4.5	Certificate Revocation	42
4.5.1	Circumstances for Revocation.....	42
4.5.2	Who Can Request a Revocation	43
4.5.3	Who May Revoke Signature Holder Certificates	44
4.5.4	Revocation Request Procedure.....	44
4.5.5	Notice of Revocation.....	45
4.6	Certificate Suspension.....	45
4.7	Certificate Status Information Functions.....	45
4.8	Sequestration of Keys and Escrow	46
5	Facility Management and Operational Controls	47
5.1	Physical Controls	47
5.1.1	Site Location	47
5.1.2	Physical Access.....	47
5.1.3	Power and Air Conditioning.....	48
5.1.4	Exposure to Water Damage.....	48
5.1.5	Fire Prevention and Protection	49
5.1.6	Media Storage	49
5.1.7	Waste Disposal	49
5.1.8	Off-site Backup	49
5.1.9	Disaster Recovery	49
5.2	Procedural Controls	49
5.2.1	Trusted Roles.....	50
5.2.2	Number of Persons Required per Task	51
5.2.3	Identification and Authentication for Each Role.....	51
5.2.4	Roles Requiring Separation of Duties	51
5.2.5	Risk Analysis	51
5.3	Personnel Controls	52
5.3.1	Qualifications, Experience, and Clearance Requirements	52
5.3.2	Background Check Procedures.....	52
5.3.3	Training Requirements	52
5.3.4	Retraining Frequency and Requirements	52
5.3.5	Job Rotation Frequency and Sequence.....	52
5.3.6	Sanctions for Unauthorized Actions	53
5.3.7	Independent Contractor Requirements.....	53
5.3.8	Documentation Provided to Personnel	53
5.4	Auditing Procedure (Processing Log)	53
5.4.1	Types of Events Recorded.....	53
5.4.2	Frequency of Processing Log	54
5.4.3	Retention Period for Audit Logs.....	55

5.4.4	Protection of Audit Logs	55
5.4.5	Audit Log Backup Procedure	55
5.4.6	Notification of Recorded Events Sent to the Originating Source	55
5.4.7	Vulnerability Assessments.....	55
5.5	Records Archival.....	55
5.5.1	Types of Records Archived	55
5.5.2	Archive Retention Period	56
5.5.3	Protection of Archives.....	56
5.5.4	Requirements for Timestamping of Records.....	56
5.5.5	Archive Collection System.....	56
5.5.6	Procedures for Obtaining and Verifying Archive Information	56
5.6	Key Changeover.....	56
5.7	Compromised Keys and Disaster Recovery	57
5.7.1	Incident and Compromised Key Handling Procedures	57
5.7.2	Corrupted Computing Resources, Software and/or Data (Equipment, Software and/or Data) 57	
5.7.3	Compromised Private Key Procedures for Entities	57
5.7.4	Business Continuity Capabilities after a Disaster	57
5.8	Termination of Activities	58
5.8.1	CA Termination	58
5.8.2	C/RSP Termination	58
5.8.3	LRA Termination	59
5.8.4	End of Life of the PKI	59
6	Technical Security Controls	60
6.1	Key Pair Generation and Installation.....	60
6.1.1	Key Pair Generation	60
6.1.2	Private Key Delivery to Subscribers	61
6.1.3	CA Public Key Delivery to Certificate Users	61
6.1.4	Key Size.....	61
6.1.5	Generating Public Key Parameters and Quality Control.....	61
6.1.6	Key Usage.....	62
6.2	Protection of Private Keys and Cryptographic Modules.....	62
6.2.1	Cryptographic Module Standards and Controls	62
6.2.2	Protection of the CA’s Private Keys (and their control by multiple individuals)	62
6.2.3	Private Key Escrow	62
6.2.4	Private Key Backup	62
6.2.5	Private Key Archiving.....	62
6.2.6	Private Key Transfer into or from a Cryptographic Module	62
6.2.7	Private Key Storage in the Cryptographic Module	63
6.2.8	Multi-user Control (m of n)	63
6.2.9	Protecting Subscribers’ Private Keys	63
6.2.10	Private Key Activation Method	63
6.2.11	Private Key Deactivation Method	64
6.2.12	Private Key Destruction Method	64
6.2.13	Evaluation of the Cryptographic Module.....	64
6.3	Other Aspects of Key and Certificate Management	65
6.3.1	Public Key Archival	65
6.3.2	Certificate and Key Usage Periods.....	65
6.4	Activation Data	65
6.4.1	Activation Data Generation and Installation.....	65
6.4.2	Activation Data Protection.....	66
6.4.1	Other Aspects of Activation Data	66

6.5	Computer Security Controls	66
6.6	Control Measures.....	67
6.7	Network Security Controls.....	68
6.8	Timestamping and Dating System	68
7	Certificate, CRL, OCSP and TSA Profiles.....	69
7.1	Certificate Profile.....	69
7.2	CRL Profile	78
7.3	OCSP Profile	81
7.4	TSA Profile	82
8	Compliance Audit and Other Assessments.....	84
8.1	Frequency and/or Circumstances of Assessments	84
8.2	Identity/Qualification of Assessor	84
8.3	Assessor’s Relationships to Assessed Entity	85
8.4	Topics Covered by the Assessment	85
8.5	Actions Taken as a Result of Deficiency	85
8.6	Communication of Results.....	85
9	Other Business-Related and Legal Matters	86
9.1	Fees.....	86
9.1.1	Subscription Fees.....	86
9.1.2	CRL Access Fees and Certificate Status	86
9.1.3	Identity Verification Fees	86
9.1.4	Fees for Other Services.....	86
9.1.5	Refund Policy	86
9.2	Financial Responsibility	87
9.2.1	Insurance Coverage.....	87
9.2.2	Other Assets.....	87
9.2.3	Insurance or Warranty Coverage for User Entities	87
9.3	Confidentiality of Professional Information.....	87
9.3.1	Scope of Confidential Information.....	87
9.3.2	Information Not Within the Scope of Confidential Information	88
9.3.3	Responsibility to Protect Confidential Information	88
9.4	Protection of Personal Information.....	88
9.4.1	Privacy Plan	88
9.4.2	Information Deemed Private	88
9.4.3	Information Not Deemed Private.....	88
9.4.4	Responsibility to Protect Private Information.....	88
9.4.5	Notice and Consent to Use Private Information	88
9.4.6	Disclosure Pursuant to Judicial or Administrative Process	88
9.4.7	Other Information Disclosure Circumstances.....	88
9.5	Intellectual Property Rights.....	89
9.6	Representation and Warranties.....	89
9.6.1	Regarding Information Contained in Certificates.....	89
9.6.2	Regarding Information in the Repository	89
9.7	Limitations of Warranties.....	89
9.8	Limitations of Liability	89
9.9	Indemnification	90
9.10	Approval Procedures	90
9.10.1	CP Approval Procedure	90
9.10.2	CPS Approval Procedure.....	90
9.10.3	Term of Validity	90
9.11	Individual Notices and Communications with Participants	90
9.12	Amendments.....	91

9.13	Dispute Resolution Provisions	91
9.14	Governing Law	92
9.15	Interpretation.....	92
9.15.1	Applicable Laws.....	92
9.15.2	Validity of Provisions	92
9.16	Force majeure	93
9.17	Review	93
9.18	Effective Date	93

1 General Provisions

1.1 Overview

The mission of Solutions Notarius Inc. (hereinafter “Notarius”) is to provide digital and electronic signature solutions that ensure the long-term reliability of documents.

Notarius also offers its clients a solution for securing documents by barcode, the visible digital seal (VDS), which includes electronically signed key data to detect any alteration and to confirm the authenticity and legitimacy of the issuer.

Notarius has also been a trusted service provider serving professionals and their business partners for many years.

Notarius is the only company in Canada to certify trusted identities and professional status, issuing trusted digital signatures recognized by both Adobe and Microsoft.

Notarius’s Public Key Infrastructure (PKI) allows not only the issuance of keys and certificates for signing electronic documents, but also the encapsulation of key data.

We can therefore say that:

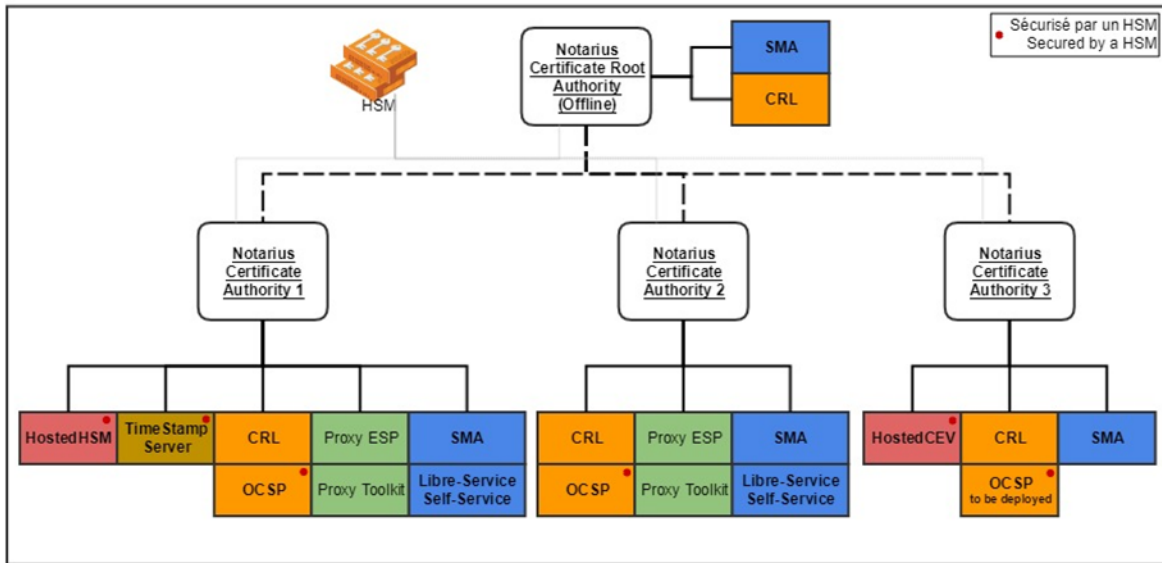
- A Notarius digital signature certifies the signer’s professional status or employment affiliation.
- The digital signature’s integrity protects the document’s content against unauthorized changes.
- Encapsulation guarantees the origin and integrity of key document data.

This CPS describes the procedures and requirements used by the Certification Service Provider/Repository Service Provider (CSP/R) to issue and manage qualified and advanced digital signatures and visible electronic seals (VECs) of the PKI in accordance with the Certificate Policy (CP). The CPS therefore describes not only the service and infrastructure management, operations and procedures for creating, issuing, managing and using certificates, but also the requirements for verifying the identity of the holders and the stakeholders involved

This CPS complies with the principles and recommendations defined in ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 & ETSI EN 319 412-3 standards.

This CPS also complies with the standards and recommendations made by the AIGCEV (International Association for the Governance of Visible Digital Seals) for the issuance of VDSs because Notarius holds several PKIs. The scope of this CPS is only limited to Notarius's PKIs commonly known as iCA1, iCA2 and, iCA3.

Notarius Certificate Authority



1.2 Document Identification and Object Identifier Numbers (OID)

The Certification Practices Statement complements the Notarius CP.

It is identified in particular by its object identifier number (OID) as follows: 2.16.124.113550.2

The OIDs for the Notarius PKI consist of the following:

Description	Object Identifier (OID)
Root CA certificate / <i>Certificat de l'AC Racine: Notarius Root Certification Authority</i>	2.16.124.113550.2.1
Issuing CA certificate / <i>Certificat de l'AC émettrice: Notarius Certificate Authority</i>	2.16.124.113550.2.2
<ul style="list-style-type: none"> Identify verification level / <i>Niveau d'assurance de l'identité</i> 	2.16.124.113550.2.2.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Identity NOT verified / <i>Identité NON vérifiée</i> 	2.16.124.113550.2.2.1.0
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Test/demo certificate / <i>Certificat de test/démo</i> 	2.16.124.113550.2.2.1.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> 	2.16.124.113550.2.2.1.1
<ul style="list-style-type: none"> Types of identities certified / <i>Nature d'identités certifiées</i> 	2.16.124.113550.2.2.2
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Natural person / <i>Identité d'un individu physique</i> 	2.16.124.113550.2.2.2.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Legal person / <i>Personne morale</i> 	2.16.124.113550.2.2.2.2
<ul style="list-style-type: none"> Minimum support required / <i>Support minimum requis</i> 	2.16.124.113550.2.2.3
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Software support / <i>Support logiciel</i> 	2.16.124.113550.2.2.3.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Cryptographic support required / <i>Support cryptographique requis</i> 	2.16.124.113550.2.2.3.2

<ul style="list-style-type: none"> • Specific functions / <i>Fonctions spécifiques</i> 	2.16.124.113550.2.2.4
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Intended for server automation / <i>Pour serveur automatisé</i> 	2.12.124.113550.2.2.4.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Complies with Adobe Approved Trust List (AATL) / <i>Conforme à Adobe Approved Trust List (AATL)</i> 	2.16.124.113550.2.2.4.2
Issuing CA 2 certificate / <i>Certificat de l'AC émettrice 2: Notarius Certificate Authority 2</i>	2.16.124.113550.2.3
<ul style="list-style-type: none"> ▪ Identify verification level / <i>Niveau d'assurance de l'identité</i> 	2.16.124.113550.2.3.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Identity NOT verified / <i>Identité NON vérifiée</i> <i>Certificat de test / Démo</i> 	2.16.124.113550.2.3.1.0
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> 	2.16.124.113550.2.3.1.1
<ul style="list-style-type: none"> ▪ Types of identities certified / <i>Nature d'identités certifiées</i> 	2.16.124.113550.2.3.2
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Natural person / <i>Identité d'un individu physique</i> 	2.16.124.113550.2.3.2.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Legal person / <i>Personne morale</i> 	2.16.124.113550.2.3.2.2
<ul style="list-style-type: none"> ▪ Minimum support required / <i>Support minimum requis</i> 	2.16.124.113550.2.3.3
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Software support / <i>Support logiciel</i> 	2.16.124.113550.2.3.3.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Cryptographic support required / <i>Support cryptographique requis</i> 	2.16.124.113550.2.3.3.2
<ul style="list-style-type: none"> ▪ Specific functions / <i>Fonctions spécifiques</i> 	2.16.124.113550.2.3.4
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Intended for server automation / <i>Pour serveur automatisé</i> 	2.16.124.113550.2.3.4.1
Issuing CA 3 certificate / <i>Certificat de l'AC émettrice 2: Notarius Certificate Authority 3</i>	2.16.124.113550.2.4
<ul style="list-style-type: none"> ▪ Identify verification level / <i>Niveau d'assurance de l'identité</i> 	2.16.124.113550.2.4.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Identity NOT verified / <i>Identité NON vérifiée</i> <i>Test/demo certificate / Certificat de test/Démo</i> 	2.16.124.113550.2.4.1.0
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> 	2.16.124.113550.2.4.1.1
<ul style="list-style-type: none"> ▪ Types of identities certified / <i>Nature d'identités certifiées</i> 	2.16.124.113550.2.4.2
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Natural person / <i>Identité d'un individu physique</i> 	2.16.124.113550.2.4.2.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Legal person / <i>Personne morale</i> 	2.16.124.113550.2.4.2.2
<ul style="list-style-type: none"> ▪ Minimum support required / <i>Support minimum requis</i> 	2.16.124.113550.2.4.3
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Software support / <i>Support logiciel</i> 	2.16.124.113550.2.4.3.1
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Cryptographic support required / <i>Support cryptographique requis</i> 	2.16.124.113550.2.4.3.2
<ul style="list-style-type: none"> ▪ Specific functions / <i>Fonctions spécifiques</i> 	2.16.124.113550.2.4.4
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ○ Intended for server automation / <i>Pour serveur automatisé</i> 	2.16.124.113550.2.4.4.1
Other OIDs and substructures used / <i>Autres OID et sous-structures utilisées</i>	

AIGCEV	
▪ Root / <i>Racine</i>	1.3.6.1.4.1.51528
▪ Security	1.3.6.1.4.1.51528.1
○ Authorized-use	1.3.6.1.4.1.51528.1.1
▪ Test-certificate	1.3.6.1.4.1.51528.2.1
▪ Vds-signature	1.3.6.1.4.1.51528.2.2
Adobe	1.2.840.113583
▪ Acrobat	1.2.840.113583
▪ Acrobat Security	1.2.840.113583.1
▪ pdfX509Extension	1.2.840.113583.1.9
○ pdfTimestamp	1.2.840.113583.1.9.1
▪ Intended for Adobe / <i>Pour test Adobe</i>	1.2.840.113583.1.2.2
Microsoft	1.3.6.1.4.1.311
▪ Timestamping	1.3.6.1.4.1.311.3
▪ Microsoft ISPU Test	1.3.6.1.4.1.311.19
IANA (<i>Internet Assigned Numbers Authority</i>)	
▪ Iana Security-related objects	1.3.6.1.5
▪ Mechanisms	1.3.6.1.5.5
▪ PKIX	1.3.6.1.5.5.7
▪ Private certificate extensions	1.3.6.1.5.5.7.1
○ AuthorityInfoAccess (AIA) <i>OCSP URL</i>	1.3.6.1.5.5.7.1.1
▪ Extended key purpose OIDs	1.3.6.1.5.5.7.3
○ Timestamping	1.3.6.1.5.5.7.3.8
○ OCSP Signing	1.3.6.1.5.5.7.3.9
▪ Access descriptors	1.3.6.1.5.5.7.48
○ OCSP	1.3.6.1.5.5.7.48.1
○ OCSP-nocheck	1.3.6.1.5.5.7.48.1.5

1.3 Definitions and Abbreviations

1.3.1 Abbreviations

- **AATL:** Adobe Approved Trust List
- **AIGCEV:** International Association for the Governance of Visible Digital Seals
(*Association internationale de gouvernance du cachet électronique visible*)
- **ARL:** Authority Revocation List

- **AVA:** Affiliation Verification Agent
- **CA:** Certification Authority
- **C/RSP:** Certification and Repository Services Provider
- **CN:** Common Name
- **CP:** Certificate Policy
- **CPS:** Certification Practices 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
- **RPA:** Recognized Professional Association
- **RPO:** Recovery Point objective
- **RTO:** Recovery Time objective
- **SLA:** Service Level Agreement
- **VDS:** Visible Digital Seal

1.3.2 Definitions

The terms used in this CPS have the following meanings:

- **Activation:** Operation performed by the subscriber and consisting of registering activation data using a cryptographic device to generate the subscriber’s certificates.
- **Activation data:** Information needed to activate keys and certificates that the subscriber must protect to ensure confidentiality (e.g., a PIN).
- **Attribution:** Issuance of keys and certificates to an applicant.
- **Audit:** An independent monitoring of a system’s records and activities conducted by a competent and impartial agent to assess the suitability and effectiveness of system controls, ensure compliance with established operational policies and procedures, and recommend necessary modifications to controls, policies, or procedures.
Audits assess the management process put in place by the C/RSP or LRA to identify weaknesses and/or nonconformity. Audit findings enable the C/RSP and LRA to take the appropriate actions to correct all observed shortcomings and malfunctions.
- **Authentication:** Process to verify the declared identity of a subscriber (individual or organization) in order to grant the subscriber access to resources (systems, networks, or applications).
- **Automated approval and revocation process:** Service that allows a professional association to automate the approval stage of applications for professional digital signature applications

from its members or the revocation of such applications based on the transmission and processing of data directly from the association's registry, provided to Notarius on a daily basis.

- **Business partner:** A legal person that wishes to perform electronic transactions with subscribers. It must be authorized to do so and have an agreement to this effect in place with the C/RSP.
- **Buyer:** The person who initiates the subscription process for one of Notarius's Products, for themselves 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 or a legal person or to the hardware or software element 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 Practices Statement (CPS):** Document that establishes and details the organizational, procedural, operational, technical, and human practices observed by the C/RSP in order to provide certification services in accordance with its binding CP.
- **Client application:** An application or software program installed on the subscriber's workstation or accessed online through which the subscriber can activate or recover certificates, change their password, perform configuration tasks, or make transactions using their certificates.
- **Compromise:** A confirmed or suspected security policy breach in which unauthorized disclosure or loss of control over sensitive information may have occurred. With respect to private keys, a compromise may include the loss, theft, disclosure, modification, or unauthorized use of a private key, or any other event compromising the integrity of a private key.
- **Confidentiality:** Information property that may only be made available or disclosed to authorized individuals, entities, or processes.

- **Customer Relationship Management (CRM):** A management tool used by the C/RSP to capture, process, and analyze information about clients, partners, employees, or prospects.
- **Device:** Application authorized by the C/RSP that permits the comprehensive or partial management of a subscriber's keys and certificates, including but not limited to their activation, renewal, and recovery. A device may be a software program, transaction platform, or web service.
- **Digital Signature (DS):** The private and public keys contained in a certificate issued to a Holder for the purpose of identifying them in the context of their use of the Products. Certificates include all information confirming the Holder's identity. Notarius cryptographically links an official identity to the Digital Signature certificate protected by two-factor authentication that is securely delivered to a validated user. Digital Signatures issued by Notarius can be affixed to PDF, PDF/A, and any other type of supported documents. The types of Digital Signatures vary according to the product(s) to which the user has subscribed. A Digital Signature remains valid until it expires or is revoked.
- **Escrow:** or "escrow agreement" consists of a supplier of a product or service entrusting a third party with the escrow of essential elements (software, databases, documents, etc.) for the use of this product or the realization of this service. The objective is to ensure that a third party (customer, partner, etc.) can access them, according to the provisions agreed between the parties, and in particular in the event of the supplier's failure.
- **Hardware Security Module (HSM):** Hardware cryptographic device in which certification authorities' public and private keys are stored.
- **Holder:** An organization, legal entity or 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, authenticate, and/or encrypt documents according to its needs or available functionalities. Holders are duly authorized end users of one of Notarius's products; they may be the holder of a certificate that will be assigned either to a group, a device or an application.
- **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**), the point to which information used by an activity is to be restored to enable the activity to operate upon resumption.
- **Modification:** Action performed with the intent to correct the information contained in a certificate by attributing a new, modified certificate.
- **Personal Information:** Any information or information of a personal nature that relates to an individual and allows that individual to be identified. Personal Information collected by Notarius to ensure that the digital signature certificates issued are valid and reliable may

contain first and last names, contact information, and photocopies of valid government-issued proof of identity for identification purposes. The collection, retention, use, disclosure and destruction of this information is carried out in accordance with applicable laws and regulations on the protection of personal information, including the laws protecting personal information in Quebec and Notarius's certification policies, as well as Notarius's Privacy Policy. Personal Information kept by Notarius is locally encrypted, protected against hackers, and protected against data loss as well as unauthorized internal use. Personal Information may only be accessed by specific Notarius officers in special circumstances such as a doubt as to the validity of the issuance of a digital certificate or a court order or order for the disclosure of Personal Information.

- **Policy Object Identifier (Policy OID):** Numerical designation contained in the certificate that refers to the CP and makes it possible to establish the certificate's trust level.
- **Private key:** The key in a subscriber's asymmetric key pair that must be used only by the subscriber.
- **Public key:** The key in an entity's asymmetric key pair that can be made public.
- **Public Key Infrastructure (PKI):** Set of physical components, functions, and procedures performed by software and human resources to manage keys and certificates issued by the CA.
- **Reattribution:** The attribution of new certificates to the same subscriber following the revocation or non-renewal of their certificates.
- **Recognized Professional Association (RPA):** A legally constituted professional association expressly dedicated to safeguarding the public interest, with which members of a given profession are affiliated and which enjoys government-sanctioned prerogatives such as regulatory and disciplinary powers. All professional associations governed by Quebec's *Professional Code* are deemed RPAs.
- **Recovery:** Action performed at the request of the subscriber or the C/RSP to regenerate the subscriber's keys and certificates when they cease to function, particularly due to a technical problem, the accidental destruction of a user's profile, or a forgotten password.
- **Recovery Time Objective (RTO):** Period following an incident within which a product or service or an activity is resumed, or resources are recovered.
For products, services and activities, the recovery time objective is less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.
- **Third Party:** Any person who relies on a certificate issued under the PKI. A third 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.
- **Subscription:** The subscription to one or more Notarius Products to which the Holder or the Buyer has subscribed.
- **Subscription Fees:** The Subscription Fees that the 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.
- **Visible Digital Seal (VDS):** Device that guarantees the origin and integrity of a document's key data by encapsulating the data, along with a user's digital signature for their organization or department, in a two (2) dimensional code. The VDS to which this CP refers is the **Otentik VDS**, whose governance is dictated by AIGCEV.
- **VDS Verification Application:** The application used by the user to verify the VDS of data received from the server public key contained in the certificate.

1.4 Interpretation

This CPS is derived from the CP which is 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

The practices referred to in this document explained here in detail with a view to meeting industry requirements.

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, ETSI EN 319 411-2 and ETSI EN 319 412-3 standards.

For enhanced clarity, the structure of this CPS 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 President, acts as a Certification Authority (CA).

In this role, Notarius undertakes to:

- Issue certificates in compliance with the CPS and 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 following: Chief Executive Officer of Notarius; Vice

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

President, Finance and Administration (also the PKI Officer); Vice President, Sales and Marketing.

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 the CA;
- Develop and update the CPS in accordance with CP requirements;
- Identify and nominate the principal actors of the PKI, including the PKI Officers;
- 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 the CA's 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;
- Delegate certain functions to the designated Local Registration Authorities (LRAs).

1.6.3 Local Registration Authority (LRA)

1.6.3.1 Definition

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

The LRA may be a Recognized Professional Association (RPA), such as a professional association or 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 it has delegated and authorized to do so (*see the excerpt from the Board of Directors' minutes from February 25, 2015): CA-2015-1-10.1 Affaires diverses*).

- The signed contractual agreements are filed here: **Contractual Agreements** (electronic versions).
- The original paper versions, when available, are filed in a vault (black fireproof filing cabinet) with restricted access near the office of the Vice-President of Finance and Administration.
- For tracking purposes, records of the signed agreements are documented in Podio in the legal area <https://podio.com/notariuscom/affaires-juridiques/apps/contrats-ententes> and in

an area dedicated to professional associations <https://podio.com/notariuscom/ordres-et-association>

1.6.3.3 Roles and Responsibilities of LRAs

The LRA formally delegates its authority to Affiliation Verification Agents (AVAs) for businesses or professionals that it has expressly identified to the C/RSP. AVAs must also complete the appointment forms, where applicable:

- Corporate AVA (identified in the account opening form): **Billing account form**
- Corporate AVA: **Appointment Form AVA-Organization_interactive.pdf**
- Professional AVA - nomination: **Appointment Form AVA-Pro_interactive.pdf**
- Professional AVA - appointment: **Commitment Form AVA-Pro_interactive.pdf**

The LRA must:

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

The LRA or its AVA must:

- Apply and comply with the CP, CPS, and all established procedures for using the management portal, where applicable;
- Approve or reject the registration of initial certificate applications submitted to it by confirming the applicant's registration in their professional association's registry (and the accuracy of all information provided concerning the applicant's name) or that the applicant is employed by the LRA;
- Revoke the professional digital signature of any holder who no longer meets the requirements of their professional association within a maximum of 24 hours between receipt of the request for revocation and the decision to modify the information on the status of the request;
- Request that the C/RSP revoke, when necessary, the corporate digital signatures of its employees from its corporate account;
- Unless otherwise provided in a 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, group, or an entity/group/application (for example, with respect to certificates for departments) that uses its certificate to sign, authenticate itself, and/or encrypt documents according to its needs or the functions available to it.

The holder is a duly authorized end user of one of Notarius's products;

1.6.4.2 Roles and Responsibilities

As use of the CertifiO for Employees or CertifiO for Professionals digital signature is a personal right, it is strictly forbidden to entrust or disclose the information allowing its use to anyone whomsoever. In addition, as the use of the CertifiO for Departments or CertifiO for Organizations digital signature is a personal right, it is strictly forbidden to entrust or disclose the information allowing its use to anyone whomsoever who is not authorized within the identified department or organization under penalty of immediate revocation.

At all times, subscribers must:

- Comply with all applicable terms and conditions of the [CP](#) and CPS;
- Respect the [General or Specific Conditions of Use of Notarius Products](#) available at all times on its website;
- Fulfil the subscription requirements ([How to sign up in 4 easy steps](#)) stipulated by the C/RSP, specifically by following [the subscription process for the product selected](#), available at all times on the Notarius website; in particular by filling out the dedicated form and entering his personal information, including his professional e-mail address; by proceeding with payment; by responding to the validation process for the professional e-mail address and defining his security questions before planning his face-to-face identity verification with an IVA designated by the C/RSP.
- Provide all information and documentation required by the C/RSP; including the information appearing in the digital signature properties such as first name, last name, member number (when applicable), and work email address;
- Protect the confidentiality of their activation data, authentication data, password, and private key, in addition to the equipment or media on which it is stored;
- Ensure that they are the only ones to use their certificates (for example, they must never entrust their certificates to a colleague or collaborator) or, when they are assigned to a group, device or application, to ensure that they are only used by authorized persons and systems;
- Use their certificates for the authorized purposes only;
- Sign documents online to ensure their authenticity;
- Use all computer equipment in a secure manner, specifically by logging out of digital signature sessions before leaving workstations;
- Notify the C/RSP customer service department as soon as possible at 1-855-505-7272 if the subscriber suspects that the confidentiality of their keys and certificates, or their password(s), is compromised;
- Notify the C/RSP as soon as possible of any changes, or make such required changes to their account itself, through the Self-Service option, for example, email addresses or contact information;
- Refrain from using certificates the moment they are revoked or expired.

1.6.5 Other Participants

1.6.5.1 Business Partners

A business partner is defined as a legal person that wishes to deal electronically with certificate holders.

It must be authorized to do so and have entered into 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;
- Comply with all technical and functional requirements stipulated by the C/RSP;
- Designate a person within their organization to hold PKI keys and 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 subscribers are equipped to comply with all obligations arising from the policy, including but not limited to the obligation to maintain the confidentiality of private keys;
- Notify the C/RSP of any event that may require action to be taken on keys and certificates, including their revocation.

The C/RSP may, at its discretion, require the business partner to undergo an audit or provide an audit report on pre-determined aspects

(See the model contractual agreements here: ...Documents_modèles\affaires_juridiques)

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 key or certificate subscriber/holder.

Any third-party user wishing to act based on a certificate must ensure that the certificate:

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

Third-party users wishing to act based on a VDS must also ensure that the signer had the legitimacy to sign the use case. To do so, third-party users must refer to the “Practices Statement” for the use case, which describes the process required to validate its legitimacy.

Third-party users can verify the reliability of electronic PDF documents signed using the CertifiO® digital signature or the ConsignO Cloud® electronic signature platform, or verify the reliability of printed documents that have a CertifiO® Code VDS by using [VerifiO®](#).

1.7 Use of Keys and Certificates

1.7.1 Authorized Use of Keys and Certificates

Certificates issued under this CPS 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;
- To encrypt electronic documents to ensure that information remains confidential, if applicable;
- To sign the data contained in the Otentik VDS.

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 CPS.

The following table provides a brief description of the appropriate uses of the CertifiO® digital signature types. These descriptions are for information purposes only; they can also be found on our website at www.notarius.com.

Product/Certificate Type	Appropriate Use
CertifiO for Professionals	<p>Digital signature certificate, certifying the signer’s identity and professional status. For the exclusive use of the professional named in the certificate. The member number is indicated in the certificate. Requires an agreement between Notarius and the subscriber’s professional association. Face-to-face identity verification. Certification of employment status or employment relationship.</p>
CertifiO for Employees	<p>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.</p>
CertifiO for Departments	<p>Digital signature certificate, certifying the name of the department or of the organization, and associating the signed document with the organization’s department. Certifies the authenticity of the document issued by the department or by the organization. The signature is made by an employee on behalf of the organization, for a maximum of 2,000 signatures annually. Available as a USB security token issued by Notarius. Recognized by Adobe products with no configuration necessary. These certificates can also be issued as soft tokens.</p>
CertifiO for Organizations	<p>Digital signature certificate, certifying the name of the department or of the organization, and associating the signed document with the organization’s department. To be installed on a server, usually for a large volume of documents digitally signed annually.</p> <p>Delivered through its Hosted HSM service or on USB security tokens issued by Notarius. Recognized by Adobe products with no configuration necessary.</p>
CertifiO Code	<p>A digital signature certificate signing the visible electronic stamp to ensure its integrity and authenticity. Issued for one or more specific use cases as authorized by AIGCEV.</p>

	Issued to organizations generally responsible for issuing documents to which the VDS will be affixed.
CertifiO for Evaluation	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 signer’s identity 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, service level agreements, or product specifications may limit the uses that the holder of its certificates may make, including the number of uses. All products offered by Notarius are limited to reasonable and non-abusive use that varies according to the service specifications. As an example and without limiting the scope, the use of CertifiO for Professionals, for Employees and for Departments is reserved for signers who have specific knowledge of the documents to be signed, either individually or as a batch; the use of CertifiO for Organizations is also limited to the number of signatures specified in the subscription.

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 CPS is strictly prohibited.

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

1.7.3 Authorized Holder

The authorized holder is:

- A member of an RPA who has an agreement with the C/RSP;
- An individual acting for a legal person (employee, agent, etc.) who wishes to use keys and certificates for professional purposes and on behalf of that legal person;
- An individual acting for a legal person (employee, agent, etc.) whose keys and certificates will be assigned to a group, device, or application;
- Any individual who wishes to have a certificate for their own use and who meets the requirements of the C/RSP.

1.8 CPS Management

1.8.1 CPS Manager

This CPS falls under the responsibility of Solutions Notarius Inc.

1.8.2 Contact Person

Any questions or comments regarding this CPS, the certificates issued, or any disputes should be

addressed to:
Solutions Notarius Inc.
Attn: President
465 Rue McGill, Suite 300
Montreal (Quebec) H2Y 2H1
Phone: 514-281-1577
Email: Officers@notarius.com

1.8.3 CP and CPS Approval Procedures

Notarius via its President (hereinafter the “President”) is responsible for approving the CP. 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 President 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 in both official languages.

2 Publication and Distribution of Information

2.1 Publication and Repository Responsibilities

The C/RSP is responsible for making available and publishing the CP, CPS, and the General and Specific Terms of Use of its products, as well as its RTOs and RPOs via its SLAs, on its website. It also makes information on the revocation status of valid certificates issued by the CA available to users and user applications.

The C/RSP is therefore responsible for publishing and distributing this information, based on availability requirements. For example:

- The repository where CRLs and certificate information are published is accessible online at all times for certificate holders, third-party users and any other PKI stakeholder, except during maintenance or in case of force majeure.
- The certificate repository is available based on the service level established by the C/RSP.
 - Access is free of charge when made by an individual who makes a low number of requests on a daily basis. In all other cases, access requires an agreement with the C/RSP.
 - Registrations appearing in the PKI repositories are solely used by holders and third-party users to access a holder's public key certificate and to access CRLs and ARLs.

2.2 Publication of Certification Information

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

- The CP and the CPS ([Certification Policies & Practice Statements](#));
- The CPS
- The General and Specific Terms of Use for products offered by Notarius ([Terms of Use](#))
- Service Level Agreements (SLAs) including their RPOs and RTOs ([Service Level Agreements](#))
- Certificate request forms;
- The Notarius Root Authority Root CA certificate ;
- The certificates of the issuing CAs are the Notarius Certificate Authority, increased by one digit if necessary;
- Valid and up-to-date CRLs:
 - http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl
 - http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl
 - http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl
 - http://crl1.notarius.com/crl1-ca3/crl/notarius_certificate_authority_3_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 President. It is therefore available 24 hours a day, 7 days a week.
 - Details of updates to the CP are clearly identified in the notes to readers and version history section of the CP
 - If applicable, changes to the CP that may affect the acceptance of the service by professionals will be notified to them by email in accordance with the contractual agreements in place or directly on the C/RSP website.
- 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.
 - Details of updates to the CPS are clearly identified in the notes to readers and version history section of the CPS
 - If applicable, changes to the CPS that may affect the acceptance of the service by professionals will be notified to them by email in accordance with the contractual agreements in place or directly on the C/RSP website.
- 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 of 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. ([Service Level Agreement for Notarius products](#)).

2.4 Access Controls on Repositories

All information published (par. 2.2) for certificate holders is freely accessible for reading. The CP, CPS, General and Specific Terms of Use, and the 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.

The C/RSP ensures that the integrity of the information published remains protected by:

- Preventing unauthorized write-access to its repositories;
- Digitally signing the CP and CPS with a certificate from an Issuing CA to protect their integrity and authenticity.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

Note that certain fields used by Notarius have pre-defined length restrictions (limits) on characters:

- CN (Common Name): 64
- O = (Fields certified by CRM): 64
- OU (Product Name): 64
- C: 2

3.1.2 Explicit Names

Names chosen to designate certificate holders must be meaningful.

As indicated in the table below, the common name (CN) for an individual holder is composed of the holder’s first and last names, as presented during the identity verification or indicated in their professional association’s registry, where applicable. For certificates delivered to organizations or departments, for example, the organization’s or department’s identity will be verified before the certificate is issued.

In brief, the distinguished name appearing in the certificates include:

- The holder’s name (or the name of the group, role, device, or application to which the holder wishes to assign keys and certificates);
- For holders that are members of a recognized professional association, the member number;
- For other holders, an administrative identification code;
- The name or acronym identifying the group to which the holder belongs.

3.1.2.1 CertifiO product details (AATL and non-AATL)

Product	uid (Unique ID)	cn (Common Name)	ou= (CRM-certified field)	o= (Product Name)	c=
CertifiO for Evaluation	Identifier composed of random characters	Test - Contact first name Contact last name -- Account name (Important: If a testing product, the product is Notarius Evaluation)		CertifiO Test CertifiO Test - AATL	c=CA
CertifiO for Professionals	Member no.	Contact first name Contact last name - - Professional title - Account nickname or Name in the account DN or Account name	Name in the account DN or	CertifiO Pro CertifiO Pro - AATL CertifiO Pro - Cloud	c=CA

CertifiO for Employees	Work email address	Contact first name Contact last name - Account nickname or Name in the account DN or Account name	Account name	CertifiO - Empl. CertifiO - Empl. - AATL CertifiO - Empl. - Cloud	c=CA
CertifiO for Departments	Identifier composed of random characters	Department name -- Account nickname or Name in the account DN or Account name		CertifiO - Dept. CertifiO - Dept. - AATL CertifiO - Dept. - Code	c=CA
CertifiO for Organizations	Identifier composed of letters and numbers	Account nickname or Name in the account DN or Account name or Name specified by client* <i>(* In the case of a name specified by the client, double dashes are not accepted if the user wishes to see the full display name.</i>		CertifiO - Org CertifiO - Org - AATL CertifiO - Org - Code	C=CA

3.1.2.2 Examples

Product	Example	DN Result
CertifiO for Evaluation - Notarius Internal Tests	Test signature for the SAC	uid=12345+cn=Test - Julien Gil -- Solutions Notarius, ou=Solutions Notarius, o=CertifiO Test, c=CA
CertifiO for Evaluation - General	Test signature for a client not identified in the CRM Testing product	uid=12345+cn=Test - Monsieur Untel -- Notarius Évaluation, ou=Notarius Évaluation, o=CertifiO Test, c=CA
CertifiO for Professionals	Signature for an engineer	uid=101010+cn=Patrick Drolet -- ingénieur - OIQ, ou=OIQ - Ordre des ingénieurs du Québec, o=CertifiO Pro, c=CA
CertifiO for Employees	Employee signature	uid=mathieu.fortin@notarius.com+cn=Mathieu Fortin -- Solutions Notarius, ou=Solutions Notarius, o=CertifiO - Empl. - AATL, c=CA
CertifiO for Departments	Signature for a Marketing Department	uid=D2A585ED+cn=Marketing -- Solutions Notarius, ou=Solutions Notarius, o=CertifiO - Dept. - AATL, c=CA

CertifiO for Organizations - server	SAC email signature on a token	Service à la clientèle -- Solutions Notarius, ou=Solutions Notarius, CertifiO - Org - AATL, c=CA
-------------------------------------	--------------------------------	--

3.1.3 Anonymization or Use of Pseudonyms

Pseudonyms are not allowed in the certificates issued.

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 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 signs or other signs, or domain names.

3.2 Identity Validation

The C/RSP 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”).

While not all ID documents are equally reliable, they all imply that the issuer verified the identity of the requester in some way before issuing the document.

“Fair,” “Strong,” and “Superior” identity document types must always have been issued by a recognized government entity:

- “Strong” or “Superior”: must have been issued as part of citizen services, not employee services (i.e., a government employee ID card is not permitted).
- “Fair”: may be a government employee ID card if and only if the C/RSP is confident that the government entity verified the employee’s identity before issuing the ID. Therefore, it was decided that only federal or provincial governments (or state governments in the United States) and government agencies or corporations would qualify.

See the **frame of reference for individual identity verifications** completed by the C/RSP. The identity of an applicant is always verified by an authorized person in accordance with the **Business Rules for Identity and Affiliation Verifications**.

The following principles apply:

- The **identity verification (IV)** must be completed by an IVA authorized by the C/RSP:
 - Remotely by an employee authorized by Notarius according to the **documented procedures**.
 - In person by an employee authorized by a legal person who has signed a written agreement with Notarius (**exception procedure**)
- The **affiliation verification (AV)** must be completed by an AVA for companies or professionals whose powers have been formally granted by their LRE. The LRE is required to formally authorize and identify its AVAs with Notarius.
 - The **AVA nomination procedure** must be followed.
 - The necessary **forms** must be completed, signed and returned to the C/RSP.
- The person who completes the identity verification for a client may not also serve as the identity confirmation agent for that same client.

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

The Notarius PKI business rules stipulate the verifications required for each product or certificate requested:

<i>Product Activity</i>	CertifiO for Professionals	CertifiO for Employees	CertifiO for Organizations	CertifiO for Departments	CertifiO for Evaluation
<i>IV Type</i>	DI or TR	DI or TR	Enterprise verification (no IV for the applicant)	Enterprise verification (no IV for the applicant)	None
<i>AV Type</i>	Professional association	Employer	Enterprise	Enterprise	None

Key:

IV Type

- DI = Remotely with data crossover
- TR = Trusted Responder (for example, a Notarius employee or a notary holding a Notarius digital signature)

3.2.1 Initial Identity Verification

The initial identity verification process only begins once the holder has, in this order:

- Filled out the online application form
- Agree to the General Terms and Conditions of Use of the Product

- Paid related fees
- Have PSC/R confirm/validate his professional e-mail address.
- Defined its Security Questions by replying the PSC/R's email validating his business email.
- Scheduled its identity verification.

The initial identity verification is required:

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

The identity verification processes are explained in our Wiki here: ***Identity verification activities***

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 first name(s), last name(s), date of birth, photograph and signature. The second or third document (if required), which serves to increase the level of confidence and not to ensure accuracy, should include at least the first name(s) and last name(s). See the ***IV acceptance rules*** for IVAs within the C/RSP.

Identity-related information about the applicant that is included in the certificate must match the information presented as part of the identity verification process, meaning, the information provided on the membership form or the information in the professional association's registry for CertifiO for Professionals signatures.

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, the common name, or the name in the association's registry.

The initial application for keys and certificates always requires an identity verification of the applicant via ***videoconference (live or by appointment)*** or ***in person*** (individually or in a ***group session***) with the C/RSP's Identity Verification Agent, except for CertifiO Test or Evaluation.

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 initial identity verification must have been completed within the past twenty-four (24) months.

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

In the case of a ***certificate assigned to a group, device, or application***, the C/RSP must first ensure the ***legal existence*** of the legal person. The Vice-President of Finance and Administration will conduct this search on the different sites dedicated for this purpose in Canada, Quebec, and elsewhere. A copy of this verification is stored in the entity's CRM account. Once completed, the C/RSP must verify the affiliation with the legal person.

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 application supporting documents (see above).

The identity verification is normally conducted via videoconference by the C/RSP's authorized IVA, [live](#), if available, or by [appointment](#).

However, in some exceptional cases, companies may request to forgo this identity verification process (by the C/RSP's authorized IVA) and instead use their own internal process (**Identify Verification — Exception Procedures**). Here, an IVA and AVA were specifically designated to the file and a form dedicated to exceptional cases (**Identity Verification Form—CertifiO for Employees/CertifiO for Professionals**) was completed. Currently, only one organization has availed itself of this exception. This exception does not apply to the issuance of products where entity verification is required.

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. The C/RSP officers are the Vice-President of Finance and Administration, the Director of Compliance and Risk Management, the Senior Advisor and the Notarius Compliance Advisor.

3.2.1.2 List of Accepted ID Documents

The supporting documents (one (1), two (2) or three (3), depending on the circumstances) must be valid and issued by a recognized government authority. Only original IDs are accepted.

A list of ID document types may be found on the Notarius website [here](#).

- The **primary document** submitted, in addition to a photograph and signature, must include the applicant's first name(s), last name(s) and date of birth corresponding to those on the future holder application web form. Here is a list of the main types of pieces of identity accepted in Canada:
 - Driver's licence or provincial ID card
 - Passport
 - Nexus card
 - Health insurance card (different from driver's licence)
 - Citizenship card
 - Permanent resident card
- The **secondary document** must reasonably (*) indicate the first and last name(s). For example:
 - All additional types of identification
 - Social insurance card
 - Government birth certificate
 - Employee card issued by a federal or provincial government authority, including government agencies and parapublic enterprises, as well as military identification cards (excludes cities and towns)
 - Hunting licence or firearm carrying license with photo

- PIV (Personal Identity Verification) or PIV-I card
- Indian status card

The C/RSP's IVA reserves the right to complete additional or subsequent verifications prior to issuing a digital signing certificate by requesting that applicants present a third identification document.

(*) The secondary document serves to increase the level of confidence and not to ensure accuracy. Therefore, certain differences from the information on the application are acceptable. In principle, all documents submitted will allow the IVA to differentiate between individuals, including homonyms, regardless of attributes (e.g., email, professional association, etc.). Any difference that leads the IVA to believe that it could be a different person will not be accepted. Therefore, the C/RSP's IVA will accept certain differences on the secondary identity documents, for example, differences between recognized governments (e.g., a second surname that is not included on the membership form or the first ID document) or differences due to social conventions (e.g., a middle name that is missing or only represented by an initial) or a minor difference in the professional association's registry (e.g., a missing letter).

Comparison criteria used by the C/RSP's IVA:

- For last names
 - Disregard punctuation (periods, apostrophes).
 - Last name(s) listed on the primary identity document must match the application.
 - Last name(s) listed on the secondary identity document must be included in the application OR the last name(s) provided in the application must be included on the secondary identity document (e.g., Caballero vs. Caballero Guerrero).
- For first names
 - Disregard punctuation (periods, apostrophes).
 - If the application does not include initials, initials on the identity documents may be disregarded.
 - If the application includes one or more initials, they must match the initials of the name(s) or corresponding initials on one of the identity documents. This includes an initial as the first name.
 - The first, middle, and last name(s) on the primary identity document must match the application, except for initials, for which the rules above apply.

3.2.1.3 Affiliation Verification by an Authorized Entity

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

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

In the automated approval and revocation process, the C/RSP accepts minor differences in first and last names between the information submitted and the information in the professional association's

registry.

- For last names
 - Accents and hyphens may be different
 - The abbreviations “St.” and “Ste.” may be used interchangeably with “Saint” and “Sainte”
 - Names with prefixes may or may not include a space (“Mc Culloch” vs. “McCulloch” or “Mac Arthur” vs. “MacArthur”)
 - Additional last names on the application listed only on the secondary identity document (common for Spanish last names)
 - An authorization from the professional association’s AVA or an officer when additional last names are only listed on the application or only on the two identity documents (common for Spanish last names)
- For first names
 - Accents and hyphens may be different
 - Compound names may or may not include a space or hyphen (“Van Deth” vs. “VanDeth” or “Marie-Anne” vs. “Marieanne”)
 - Connecting words may be disregarded (“Maria de Fatima” vs. “Maria Fatima,” common for Spanish names)
 - Additional names listed on the application are only listed on the secondary identity document (common for Spanish names)
 - An authorization from the professional association’s AVA or an officer when additional names are only listed on the application or only on the two identity documents (common for Spanish last names)

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.

Once the identity verification and confirmation of business relationship have been successfully completed, the request is finalized by the employee authorized by the C/RSP in the self-service portal. An email is automatically sent to the applicant informing them of the approval of their subscription request.

The subscriber receives a reference code and is invited to activate the certificate.

The activation data necessary to generate the holder’s certificate is provided to the holder after authentication in the CSP/R portal using security questions, known only to the holder, and collected during the subscription process.

3.2.3 *Identity Validation for Certificate Renewals*

Holders are notified in advance by email (multiple emails are sent at days 30, 15, 9, and 0) that their keys and certificates are about to expire.

Thirty (30) days before the expiration date, if the holder uses their digital signature online, the renewal is automatically completed via Entrust.

In most cases, the certificate is updated automatically.

The holder will receive a confirmation email in case of successful update.

If the automatic renewal process fails, the holder will be notified by email that the update did not work, the signature has expired, and the certificate has been revoked.

- If the holder's subscription is still active, the holder will then have to recover the certificate by self-authenticating using their keys and certificates on the C/RSP portal and by answering their security questions.
- Otherwise, in the case of an inactive or expired subscription, the holder will have no choice but to re-subscribe and complete the entire process again (i.e. identity verification and authorization from the RPA).

3.2.4 Identity Validation for a Re-key

At the C/RSP we talk internally about "re-subscription".

When the holder requests the re-issuance of its keys and certificates within twelve (12) months of their revocation, expiration, or cancellation, they must successfully authenticate their identity (using their security questions or other valid digital signatures where technology permits) on the C/RSP portal.

Failing this, applicants will be required to have their identity revalidated in accordance with the procedure described in Section 3.2.1.

Re-issues are not applicable for CertifiO for Organizations. A new issue is preferred.

3.2.5 Identity Validation for Certificate Modifications

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

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

Updating information such as first and last name(s) requires prior verification with the applicant's RPA, which must provide written confirmation of the requested changes.

Upon receipt of written confirmation from the RPA, the C/RSP's officer will then make the requested changes in the **SMA**.

See the ***procedure for modifying, correcting or changing a name*** for the full details.

For holders of certificates for organizations or departments, a formal request to the officer designated by the C/RSP (to the sales or product management department) is required in order for the C/RSP officer to proceed manually (see ***Steps to Creating a Hosted HSM - manual portion***) or ***Modify a DN***, following the usage verifications in the client's files, with the changes requested and to take the necessary actions with the IT team leader when necessary.

4 Key and Certificate Management

4.1 Key and Certificate Issuance Request

4.1.1 Authorized persons

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 or for one of its devices or applications. For devices and applications, the legal entity must designate a natural person to act as the responsible party.

4.1.2 Application Process

Buyers who wish to obtain keys and certificates for themselves or for an authorized holder must:

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

The steps in the subscription process previously mentioned are described [here](#).

The subscription process for CertifiO for Organizations differs slightly in the sense that the signing of a formal prior contractual agreement is required to initiate the subscription process (all contracts are listed by the C/RSP). The client must complete the [account opening form](#) sent by the C/RSP's sales team or administrative services department. In addition to the client, this process involves the C/RSP's sales team, the PKI Officer, and the IT and product teams.

4.1.3 Approval or Rejection of Certificate Applications

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

4.1.3.1 Approval or Rejection of a Corporate or Departmental Digital Signature Application

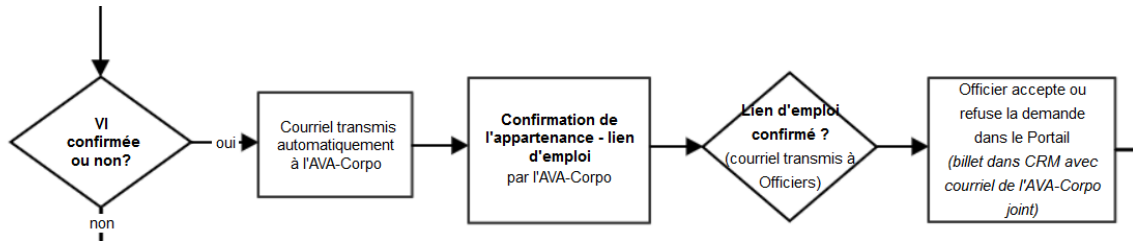
Applications for corporate or departmental signatures must be approved or rejected by the LRA's AVA, upon receipt of an email that the C/RSP automatically generates.

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, membership or employment relationship via the restricted-access Notarius digital signature management platform.

For employees digital signatures: [images for reference purposes only]



[Mon compte](#) | [Aide](#)

Lien d'emploi à confirmer

Cher AVA,

... a effectué une demande de signature numérique corporative liée à ... ou à l'une de ses unités d'affaire. Nous avons confirmé son identité ainsi que son adresse de courriel. Son identifiant unique, basé sur son adresse de courriel, sera le "

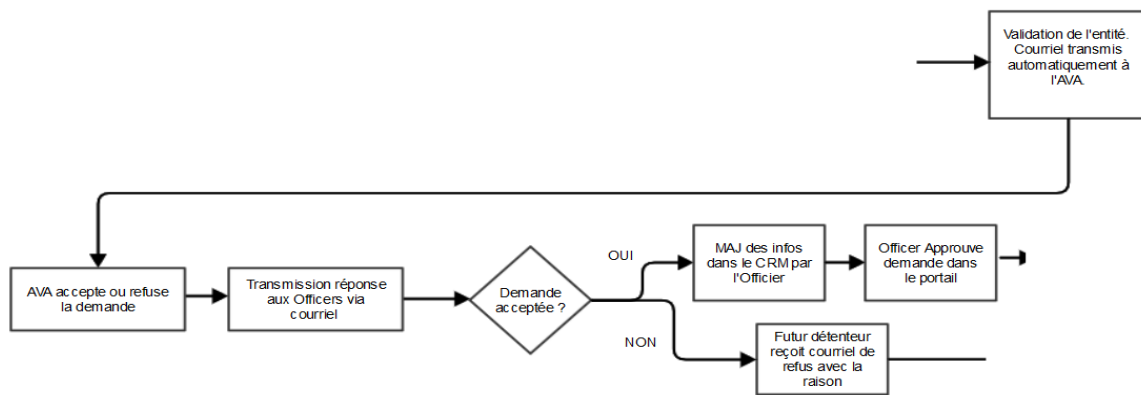
[Confirmez l'emploi \(par courriel\)](#)

[Refuser la demande \(par courriel\)](#)

Des questions?

Clavardez avec un de nos spécialistes du service à la clientèle, ouvrez un billet à www.notarius.com/aide, ou contactez-nous au 1-855-505-7272.

For department digital signatures: [images for reference purposes only]



Application to approve

Dear AVA,

... has applied for a *CertifIO for Departments* ... digital signature linked to ... or to one of its business units.

[Approve \(by email\)](#)

[Reject \(by email\)](#)

Questions?

Consult our FAQ section, chat with one of our customer service specialists or open a ticket at notarius.com/help.

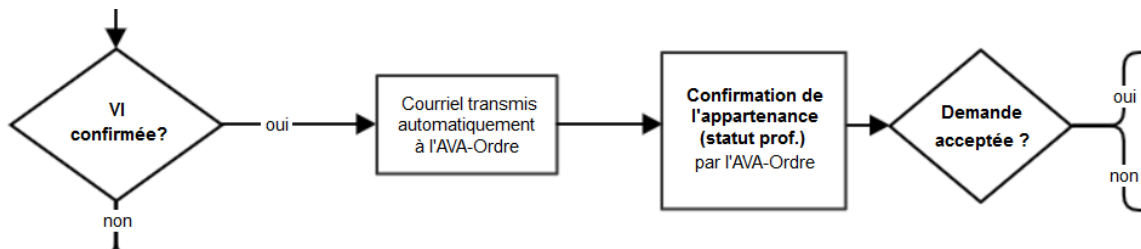
4.1.3.2 Acceptance or Refusal of an Organization's Digital Signature Application

The process always starts with the negotiation/signing of a contractual agreement. Once the agreement has been signed, the account opening form is completed, identifying the organization's authorized contacts, and signed by the account manager.

It is then sent to the accounting department for validation of the company's information (entity validation). Once all documents have been received and validated by the account VP, the C/RSP Officer can continue the certificate creation process.

4.1.3.3 Approval or Rejection of other Types of Digital Signature Applications

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



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

Three (3) types of decisions can be made:

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

Note that, in very rare cases where an RPA's AVA is not available, the RPA manager may contact the C/RSP to request that the C/RSP proceed on their behalf. A formal email, detailed list, and the cases of refusal will be required. A ticket will also be opened in the CRM with supporting documents so that the C/RSP officer may proceed on behalf of the RPA.

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

Two (2) types of decisions can be made:

1. **Approve:** Approval of the selected application, as is.

2. **Reject:** Rejection of the selected application, providing a reason (mandatory field).
- An email with the reason for rejection is immediately sent to the applicant.
 - A refund is credited to the buyer when the buyer has paid by credit card.
 - In the case of a mismatch between the personal identification information in an application and information contained in the professional association’s registry, the buyer will be invited to contact the C/RSP’s customer support department or the AVA for the registered professional association.

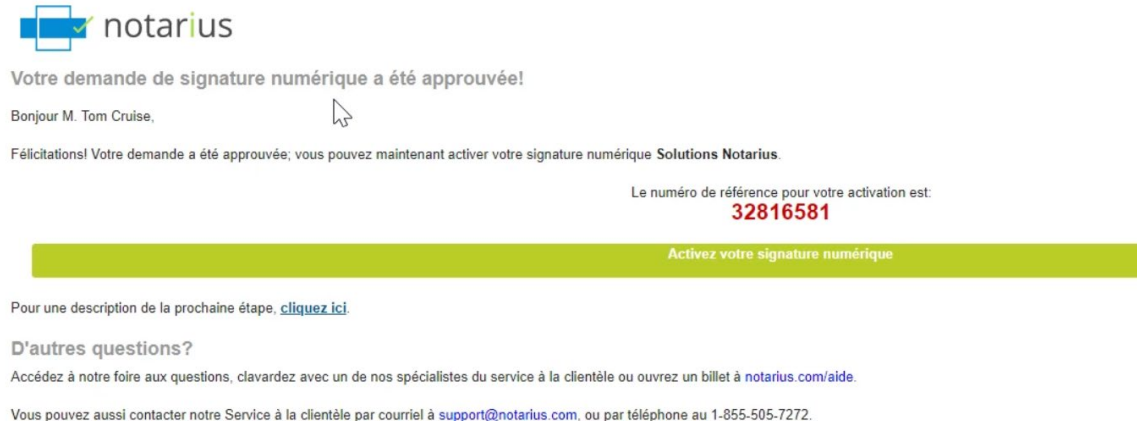
The complete details on the business rules and architecture of the new process are available [here](#).

4.1.4 Term of validity of the request

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 Approval

Subscribers will be notified by email once their application has been accepted. An AATL token will be sent to the new subscriber by registered mail, if necessary. The subscriber can then activate their digital signature once the certificate has been generated. The subscriber is deemed to have accepted the keys and certificates upon activation.



The screenshot shows an email notification from Notarius. At the top is the Notarius logo. The main text reads: "Votre demande de signature numérique a été approuvée!" followed by "Bonjour M. Tom Cruise," and "Félicitations! Votre demande a été approuvée; vous pouvez maintenant activer votre signature numérique Solutions Notarius." Below this, it states "Le numéro de référence pour votre activation est: 32816581" in red. A green button labeled "Activez votre signature numérique" is visible. At the bottom, there are links for "cliquez ici" for more details and "notarius.com/aide" for help, along with contact information for support@notarius.com and a phone number.

4.2 Certificate Renewal Requests

The certificate renewal operation is independent of the expired certificate. The renewal service also entails automatic client notifications when the private key is used in a device. A renewal consists of issuing new keys and certificates to the same subscriber using their existing private key.

During the renewal process, no new identity validation is required.

The issuing CA can renew keys and certificates provided that:

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

No additional validation or verification is necessary.

For CertifiO for Organizations, the notification is automatically sent to the C/RSP officer so that they may manually update the system certificate, when required.

4.2.1 Authorized persons

The certificate renewal process can be initiated by:

- An application;
- A device;
- The subscriber using their private key;
- C/RSP officers.

4.2.2 Certificate Renewal Procedure

Depending on the applicable certificate policies, certificates issued by the CA may be valid for 24 months, 36 months, or longer, calculated from the date of issuance. For example, an organization's certificate may be valid for 10 years and its private key for 3 years.

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

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

4.2.3 Processing Certificate Renewal Requests

Except for certificates for organizations manually processed by the C/RSP officer, the other types of certificate renewal processes are initiated automatically by the holder 30 days prior to the key's expiration date, when they use their digital signature online.

For a certificate renewal, it is necessary to:

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

4.2.4 Renewal Notice

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

The subscriber is notified by the device the moment the certificate is generated as follows:

- *30 days* before the expiration date of the private key. The holder is notified that their digital signature requires attention;
- *15 days* before the expiration date of the private key, a second notification is sent;
- *9 days* before the expiration date, the notification informs the holder that their digital signature will no longer function in nine days;
- On *day 0*, a notice informs the holder that their digital signature is no longer functional.

4.3 Certificate Recovery

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

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

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

4.3.1 Authorized persons

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 C/RSP portal (with online identity verification).

- The certificate holder must go the following link: www.notarius.com/recover
- Enter their work email address and complete the captcha;
- They will then receive a confirmation email requesting them to log in using their security questions and clicking on the button *Recover your digital signature*;
- The holder must correctly answer the security questions.
- The system automatically sends an email to the holder so that they may retrieve their certificate (the first activation code in the confirmation email and the second will be displayed on the holder's account web page after the holder has successfully completed the authentication process with their security questions).

See the following Help page: [how-to-recover-my-digital-signature-online](#)

4.3.3.2 In-person Recovery

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

4.4 Certificate Modification Requests

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

Changes to the certificate are not applicable for CertifiO for Organizations. A new issue is preferred.

4.4.1 Authorized persons

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

4.4.2 Circumstances for a Modification

A modification can be made to correct a spelling error or to change noncritical information contained in the certificate, for example, a spelling error in the first or last name, or an error in the member number or product selected.

4.4.3 Processing Certificate Modification Requests

Holders can modify certain non-critical information contained in the certificates themselves. To do so, they must first authenticate themselves using their secret questions in the C/RSP portal and make the necessary changes themselves.

Otherwise, the holder must send a written request for modification to the C/RSP so that the PKI Officer can make the requested modification(s) on the holder's behalf.

Here are a few examples of the procedures:

- **Modification, correction, or change to the client's name**
- **Modification of the member number**
- **Modification of the certificate (Change DN)**

4.4.4 Notification of Modifications

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

4.5 Certificate Revocation

4.5.1 Circumstances for Revocation

4.5.1.1 Signature Holder Certificates

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

Recording this information on the CRL indicates to third 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 holder's information contained in their 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 their certificate's applicable terms and conditions;
- The client, LRA, RPA, or CA fails to fulfil their obligations under the CP;
- A major error (intentional or unintentional) is identified in the signature holder's account information;
- The signature holder's private key is compromised or suspected of being compromised, or lost or stolen (potentially including associated activation data);
- The signature holder or an authorized person requests the revocation of the certificate (particularly in the event of destruction or damage to the subscriber's private key or the equipment on which it is stored);
- The CA's signing certificate is revoked (resulting in the revocation of all certificates signed by the corresponding private key);

- The signature holder does not accept the updated **terms of us** applicable to the product to which they have subscribed;
- The signature holder dies, or the employer ceases to operate;
- The signature holder is no longer a member in good standing of a professional association (a condition of certificate issuance);
- 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 fact (either by being notified directly or by obtaining information in the course of its verification, such as when issuing a new certificate), the certificate in question is revoked.

The CA or the C/RSP may, at its discretion, revoke a certificate when the signature holder fails to comply with the obligations set out in the CP, including the general or particular conditions of use of Notarius products. The PKI Officer will then revoke the certificate on the grounds that the subscription has expired.

Once a certificate is revoked, it cannot be reinstated.

4.5.1.2 *PKI Participant Certificates*

Various circumstances may result in the revocation of a certificate held by a particular Notarius PKI participant (including a CA 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 (e.g. following a negative result in a qualification or compliance audit);
- 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, which will immediately take necessary action.

These scenarios are evaluated and addressed in the **Notarius Business Continuity Plan—Integrity component**, as they require different action plans depending on the circumstances.

4.5.2 Who Can Request a Revocation

4.5.2.1 *Signature Holder Certificates*

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

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

As soon as a person or entity becomes aware of potential grounds for certificate revocation in an area under its responsibility, it must immediately submit a revocation request to the C/RSP's customer services department at 514-281-6533 or the compliance team at officers@notarius.com.

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:

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

4.5.4 Revocation Request Procedure

4.5.4.1 Revocation of Signature Holder Certificates

The revocation request is submitted to the issuing CA and is signed with the certificate used to make the request.

Requests to revoke certificates for organizations are processed manually after confirmation of their origin by the C/RSP Officer.

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. The same applies to OCSP responses.

A new CRL can be issued before the next scheduled CRL issuance.

As soon as the **holder** becomes aware that one of the possible grounds for revocation is effective, they must proceed without delay with their request for revocation as follows:

- By logging into the My Account section of the Notarius website;
- By communicating with the C/RSP's customer service department to open a service request in their name.

Written confirmation is required in this case and attached to the service request.

An **RPA** may revoke certificates (professional digital signatures) activated under its control by using the self-service portal, for example, when removing one of its members from the professional association's registry.

The RPA must nevertheless submit a written request to the C/RSP in order for the designated officer to manually proceed with the revocation in cases where the member's digital signature has not been activated.

The **LRA** may request via email that the C/RSP revoke corporate digital signatures under its corporate account. Most commonly, these requests are made when a holder's position is terminated.

The **PKI Officer** may revoke certificates using the C/RSP portal following the receipt of an express written request from the holder, the RPA representative, the LRA authorized representative or the employer (specifically in the cases of corporate signatures).

*See the procedures on **revoking a digital signature, converting a subscription (from a corporate to professional digital signature) and manually revoking a certificate** for more details.*

The **PKI Officer** is also responsible for revoking expired subscriptions (report produced at least once per week) in accordance with the procedure on **reporting expired subscriptions**. This is referred to as an administrative revocation of certificates.

The cause for the revocation must always be specified.

Regardless of the person who proceeds with the revocation, the reason/grounds are always recorded by the C/RSP but are not published in the CRL.

4.5.4.2 *Revocation of PKI Participant Certificates*

In the event of a contractual, hierarchical or regulatory termination between the CA and an RPA or between the CA and the LRA prior to the expiry of the certificates issued in the name of or on behalf of said RPA or LRA, all certificates must be revoked. See the ***procedure for contract termination***.

In the event that the CA ceases to operate for any reason whatsoever, Notarius undertakes (unless a contractual agreement stipulates otherwise) to provide notice without delay of the cessation of its activities and to transfer its responsibilities to the entities that will succeed it or to those designated.

Before ceasing its activities, Notarius undertakes to:

- Provide six (6) months advance notice to users and clients holding valid certificates of its intention to cease its activities as a CA;
- Give a notice of revocation to each of its clients;
- Revoke all certificates that have not yet been revoked or have not yet expired at the end of the six (6) months notice period, without further notice;
- Take all appropriate measures to preserve its archives; and
- Reserve the right to make the necessary succession arrangements for the re-issuance of certificates by a successor CA that has all the necessary authorizations to do so and that undertakes to comply with all essential rules to the extent that its operations are at least as secure as its own.

4.5.5 *Notice of Revocation*

The subscriber will receive a 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 (Added status in SMA), the subscriber will not be notified. A record of the operation will, however, be left in the contact file (CRM).

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. PKI participant certificates must be revoked as soon as an event described in the possible grounds for revocation for that type of certificate is detected. CA Server signing certificates (signing of certificates, CRL and/or OCSP responses) are revoked immediately, specifically in cases where a key has been compromised.

The procedures to be followed in the case of a revocation of a Notarius PKI Participant certificate are described in the ***Business Continuity Plan—Integrity component***.

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.

Revocation status information includes information about the status of certificates at least until the certificate expires.

This certificate status information is available 24 hours a day, 7 days a week, and without geographic restrictions.

This information provided by CRL or OCSP is consistent over time and considers the different time frames for updating status information for these two methods. However, some minor time differences can be observed between the two methods since the CRL is published directly on the Internet while the OCSP requires additional processing before publication. The registered revocation date of the certificate between the two methods will always be the same, however.

4.8 Sequestration of Keys and Escrow

The sequestration of private keys is prohibited, as are seal certificates.

An *escrow contract (class C)* is signed by the CA in the event of the cessation of its operations.

5 Facility Management and Operational Controls

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

The C/RSP uses the **risk analysis methodology** to identify risks and opportunities, and to evaluate and apply the necessary measures and controls when required.

The C/RSP holds the ISO 27001 accreditation and eIDAS certification.

5.1 Physical Controls

The C/RSP has established and maintains several policies, including an **ITC management policy**, a **comprehensive information security policy** and an **employee directive**.

These documents describe physical access controls (in this respect, the C/RSP limits access to production servers to the persons identified who require access to perform their functions), 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.

For controls and monitoring measures, see **Systems Surveillance**.

For access management, consult Section 4.4 of the **ITC management policy**, (access requests are managed in the C/RSP's **Podio** application).

For all matters related to disaster recovery processes, refer to the C/RSP's **business continuity plan**.

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 more than five kilometres away from one another geographically. For security reasons, identification information regarding the sites is classified as confidential.

These sites hold multiple certifications and 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 ensure that the provisions stipulated in the CP are respected, as well as the contractual arrangements with RPAs and LRAs and service level agreements, regarding service availability.

New colocation providers are selected according to a rigorous selection process (see **provider selection**), including site visits.

5.1.2 Physical Access

The C/RSP has defined a physical security perimeter where the hardware and software of the critical components of the PKI are installed for certificate generation and revocation management operations. Relevant internal documentation is detailed in the **Communications-Networks-Security** Wiki.

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.

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.

The PKI's computer systems are housed in facilities located several kilometres away from one another geographically. These buildings comply with applicable construction regulations and standards.

To access the premises, security and access control areas must be passed through to prevent or detect unauthorized access to systems, damages, and interference.

In addition, C/RSP has ensured that these sites meet high security requirements.

An **annual report on colocation site accesses** is sent to the C/RSP upon request for control purposes. All PKI facilities are controlled and monitored to ensure only authorized persons can access systems and data.

Here are a few examples of measures in place in at least one of the C/RSP colocation sites:

- Secure access: permanent guard posts, biometric identification and facial recognition
- 24/7 closed-circuit video surveillance
- Certification of compliance with the Payment Card Industry Data Security Standard (PCI DSS)

At the laboratory site, if unauthorized persons need to enter our facilities, they must be accompanied and supervised by an authorized person. These persons must be accompanied by authorized personnel at all times. Outside business hours, enhanced security is provided using physical and logical intrusion detection systems. **Monthly site access audits** are completed to verify site accesses.

5.1.3 Power and Air Conditioning

Power generation and protection systems are installed by the C/RSP to ensure the availability of computer systems at the PKI operating site.

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. They also fulfil the requirements of this CPS and requirements concerning operational availability.

Electrical and air-conditioning facilities ensure the proper functioning of PKI operations.

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.

Information processing redundancy is in place to ensure the availability of the primary critical systems. See the **network provider diagram** for an example.

5.1.4 Exposure to Water Damage

Sites have been built and equipped so as to ensure protection against water exposure.

Water damage prevention measures taken by our colocation providers ensure that the requirements of this CPS are met.

5.1.5 Fire Prevention and Protection

Sites have been built and equipped so as to ensure protection against fires.

These measures respect the applicable standards and laws.

Fire extinguishers and sprinklers are tested at planned intervals to ensure functionality. Reports are produced **annually** to confirm proper functioning.

5.1.6 Media Storage

Measures have been implemented to protect media containing sensitive data against damage, deterioration, theft, unauthorized access and obsolescence.

Media are handled securely depending on the information they contain.

As part of the risk analysis, media as well as the various information involved in PKI-related activities were identified and their security needs defined in terms of the availability, confidentiality, and integrity of data, in particular, data stored in the logs, archives, and software used by the CA.

Full details can be found in the **data retention policy**. Also consult the document on **backup and media management process**.

Media management procedures protect against obsolescence and deterioration of media during the records retention period - **see 10 Year Backup**.

Controls have been put in place within the C/RSP to mitigate media risks. A **comprehensive security policy**, an **employee directive** (including disciplinary measures where appropriate), and informational communications are in place.

5.1.7 Waste Disposal

To fully protect confidentiality, processes for the secure destruction of media and data in electronic format are implemented. See the **procedure for destroying sensitive information**.

These procedures ensure that the media used to store information are disposed of properly and according to the security rules in place.

Reuse of any storage media (hard drives) used by the CA for any other purpose prior to the complete destruction of any CA-related information they may contain is strictly prohibited.

Media is destroyed at the end of its service life.

Evidence of media destruction is conserved **here**.

5.1.8 Off-site Backup

Thorough 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 to ensure the fastest possible recovery following a disaster.

A description of the backups, methods used, storage locations, and more, can be found here: **Service and server backups**.

5.1.9 Disaster Recovery

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.

Backup equipment and recovery procedures are regularly tested to ensure their proper functioning.

Redundancy is also ensured for production servers.

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. They are documented in a **designated space** that can be accessed by all C/RSP employees.

Procedures are established and applied for all operations performed by personnel in trusted roles with the potential to impact on service delivery.

Operational and administrative measures and controls are implemented by the C/RSP to ensure that PKI operations remain secure.

5.2.1 Trusted Roles

The PKI administration includes trusted roles, ensuring a distribution of tasks such that there is no possible conflict of interest and no possibility of any person acting alone and circumventing the PKI security system. Full details on the trusted roles are available in the **roles matrix (PKI and SS)**.

The roles are described as follows:

- **Security Officer:** Responsible for the implementation of security practices.
- **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.
For example, the Operations Manager has access to the Security Manager and can perform digital signature registration, recovery, and revocation operations.
Currently, this role is held by the Director of Compliance and Risk Management and the Vice-President of Finance and Administration. It is the only person who can access the encrypted files of identity verification documents retained by the C/RSP.
- **PKI Administrator:** Responsible for the administration and operation of PKI systems, for example, conducting system backups and recoveries. Allowed to access PKI servers. Security Manager (SM) & Security Manager Administration (SMA).
- **Audit Log Auditor:** Authorized to perform monthly audits of PKI logs. The Audit Log Auditor has reading access only and may not modify them.
- **Self-Service (SS) Auditor:** Individual authorized to view applications for subscriptions and digital signatures issued in the SS portal.
- **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.
- **Identity Confirmation Controller (ICC) in the SS portal:** Responsible for confirming identities for subscription requests made in the SS portal.
- **Identity Verification Controller external to the SS portal:** Responsible for confirming/verifying identities in person or via a technology that has been authorized by the C/RSP.
- **Affiliation Verification Controller in the SS portal:** Responsible for confirming/approving employment affiliations in the SS portal.
- **Billing:** Person authorized to revoke corporate subscriptions linked to an account.
- **HSM Card Holder:** Responsible for keeping an HSM card required to operate the CA hardware security module.

The **trusted roles matrix** shows the distribution of functions among C/RSP resources.

Signed **confirmation forms** provide express commitment on the part of the internal resources

designated by the C/RSP.

The **IVA and AVA nomination procedure** and **Pro AVA expression of commitment** confirm their express commitment.

Any of the above-mentioned functional roles may be held by several individuals within the C/RSP. 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 in trusted roles are reviewed regularly every four years (see the **C/RSP employee directive**).

5.2.2 Number of Persons Required per Task

To ensure that a person acting alone cannot circumvent security measures and thus undermine the integrity of the service provided, the C/RSP ensures that certain tasks related to operational management are divided among several people.

However, more than one role may be assigned to the same person, as long as the combination of roles does not compromise the safety of the functions performed. Consequently, depending on the type of operations carried out, the number and type of roles, and people who must necessarily participate may be different.

In addition, certain critical tasks and activities must follow the internal procedure: see **PKI Intervention Request—Critical operations** and require the opening of tickets in Podio as well as approval from the General Director of the C/RSP, when necessary.

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 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.

The **results of the analysis as well as the statement from the ISM** are filed on the C/RSP network. This analysis is classified as confidential.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The C/RSP follows a documented **recruitment procedure** to ensure that it employs sufficient staff with the necessary knowledge, experience and qualifications to deliver PKI services.

The Vice-President of Finance and Administration (Human Resources Manager) is responsible for ensuring that duties assigned to all personnel working within the PKI correspond to their professional skills. Details are provided accordingly in all **job descriptions**.

All supervisory personnel must possess expertise appropriate to their roles and be familiar with the security procedures and privacy protection measures in force.

All individuals working at the C/RSP are subject to strict confidentiality and information security requirements, outlined in the **hiring letter** provided to every C/RSP employee.

5.3.2 Background Check Procedures

The C/RSP systematically conducts criminal background checks on all its employees in accordance with the **recruitment policy**.

Checks are also carried out at regular intervals (every four years) for all persons in a trusted role (see the **roles matrix**) within the C/RSP.

Individuals convicted of a serious crime or any other offence are not permitted to occupy a trusted role or are removed from that position immediately.

A reminder to this effect is provided in the **employee directive**.

5.3.3 Training Requirements

Immediately following their **orientation**, C/RSP employees receive training on the software, hardware, and internal operating and safety procedures.

Specifically, C/RSP employees who perform functions related to the delivery of PKI services have received appropriate training to perform their duties.

A dedicated time code has been created in the C/RSP's timesheet management portal. *Training received—PKI*

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 **escalation procedures**.

Internal training updates are given individually or as a group when there is a significant change in procedures, system developments, or an updating of trusted roles. External trainings may also be given when needed.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

The C/RSP maintains and enforces disciplinary procedures for employees who perform unauthorized actions. The disciplinary procedure described in the *employee directive (Section 8)* may include disciplinary measures up to and including termination and must take the frequency and severity of the unauthorized action into account.

Disciplinary measures are categorized from 1 to 4:

1. Verbal warning
2. Written warning
3. Suspension without pay
4. Termination

For measures 2 to 4, a note will automatically be added to the file of the employee concerned. Some examples of situations that could lead to disciplinary measures being taken against an employee include:

- Writing down a password
- Failing to lock their work sessions when stepping away from their desks
- Sending confidential information to unauthorized people
- Misuse of Notarius assets for personal purposes
- Storing or viewing pornographic materials on company assets
- Stealing company equipment or information

5.3.7 Independent Contractor Requirements

Independent contractors may not hold trusted roles in the PKI.

Requirements for independent contractors are set out in written agreements. Confidentiality agreements are systematically signed.

The C/RSP's security controls apply to all independent contractors.

Independent contractors must sign confidentiality agreements and comply with the C/RSP's security policy. External providers who work in the C/RSP's colocation centres are supervised as necessary.

5.3.8 Documentation Provided to Personnel

The C/RSP makes the CP, CPS, internal procedures, operating manuals, applicable technical documents supporting the provision of certification services, and any other relevant documents available to its staff so that it can carry out the duties it has been assigned.

This updated documentation may be found mainly on the *Wiki* and on the organization's network. In the event of a disaster, it can be accessed remotely at all times.

5.4 Auditing Procedure (Processing Log)

The *audit log* contains events that are recorded by manual entry or automatic generation.

The resulting files make it possible to trace and account for the operations carried out. A number of the C/RSP policies integrate these concepts, including the *security policy*, *employee directive*, *ICT management policy*, the *Podio incidents policy*, and the *audit log activity policy*.

5.4.1 Types of Events Recorded

The audit log contains events that are recorded by manual entry or automatic generation.

- The C/RSP records PKI-related events, including: Start-up and shutdown of computer systems and applications;

- Attempts or transactions affecting the rights and privileges of trusted roles involved in the delivery of PKI services;
- Changes to server and application passwords on PKI servers;
- Changes to the certificate creation policy;
- Denied attempts to access the PKI system;
- Changes to system security settings; and
- PKI non-compliance and security breach reports.

Other events are also recorded. They primarily concern information security, such as:

- Physical access to sensitive areas;
- System maintenance and/or configuration;
- Changes made to personnel in trusted roles; and
- Destruction of media containing confidential information.

In addition to these requirements, specific events are recorded, including:

- Receipt, approvals, or refusals of a certificate application (initial application and renewals);
- Verifications of certificate requests;
- Events related to signing keys and CA certificates (generation via the key ceremony, backup/recovery, destruction);
- Certificate generation; and
- Publication and updates to CA-related information.

The events recorded in the logs containing the following information, at a minimum:

- Type of event;
- Information identifying the executing agent and/or the reference code of the system triggering the event;
- Event date and time; and
- Result of the event.

Records may also contain the following fields, where applicable:

- Recipient of the operation;
- Name of person requesting the operation or the reference code of the system making the request;
- Names of individuals present (if the operation requires multiple people);
- Cause of the event; and
- Additional event details.

Logging operations are performed in the background throughout the life of the PKI.

Accountability for an action rests with the person, organization, or system that carried it out.

The name or identifier of the executing agent appears explicitly in one of the fields of the audit log.

Logging operations are performed in-process.

In the case of a manual entry, entries are made on the same business day as the event, except in exceptional cases.

As audit logs may contain sensitive and personal information, the C/RSP takes the necessary measures to protect the confidentiality of personal information.

5.4.2 Frequency of Processing Log

Audit logs are periodically reviewed. For examples, see this *non-exhaustive list*.

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

Processing logs under the C/RSP's management are conserved for a minimum of three (3) years in accordance with the **retention schedule**.

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. The logs may only be accessed via the Security Manager Administration (SMA) by a person authorized within the framework of their role and authenticated by their digital signature (e.g. the audit log auditor).

The logs are encrypted by the CA's certificate and are therefore unreadable outside the security manager.

Tampering with an audit log is promptly detected by integrity checks performed regularly by the CA.

5.4.5 Audit Log Backup Procedure

Personnel with specific access rights identified by the C/RSP can access audit logs. See the **roles matrix** for more information on access rights.

5.4.6 Notification of Recorded Events Sent to the Originating Source

Not applicable.

5.4.7 Vulnerability Assessments

All CA components are capable of detecting any attempt to breach the integrity of their operations. "Alarm" audit logs are analyzed monthly according to the PKI audit log procedure (see the procedure **here**). This monthly analysis verifies the concordance between different events and helps to identify all major anomalies.

Records and actions taken are stored as evidence on the C/RSP network on the **S** drive and in **Podio**. When processing information collected in the audit log that relates to system security, the C/RSP takes the necessary steps to reduce or eliminate vulnerabilities.

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. In accordance with the C/RSP's **retention schedule**, the following information is retained:

- The CP;
- The CPS;
- The General Terms of Use;
- Complete files on certificate creation requests and revocation;
- Certificates, CRL, and OCSP responses as issued or published;
- Audit logs;
- Information collected to establish a holder's identity;
- Certificates and public signing keys, as well as encryption keys and certificates;
- Data backup copies; and

- Client files.

5.5.2 Archive Retention Period

In accordance with the C/RSP's **retention schedule**, the following information is retained for the periods specified:

- 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; and
- Data backups: From 1 month to 10 years, depending on the data concerned.

A copy of the archived data is kept at a secondary site and is protected by physical and cryptographic measures. This site complies with environmental requirements, particularly with regard to temperature, humidity, and protection against magnetism.

For more information on the retention and destruction of data and media, see the **media retention and destruction policy**.

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.

The means and measures implemented to ensure that archives remain protected are specified in the procedure on **managing backups and media used**.

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. 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.

5.5.5 Archive Collection System

The system collects archive information in accordance with the appropriate security level for privacy protection. See the procedures on **managing backups and media used** and **backups and restoration**, as well as best practices on **protecting recorded information**.

5.5.6 Procedures for Obtaining and Verifying Archive Information

Archives that are physically located on C/RSP premises or on its network are immediately accessible to authorized persons.

Archives stored off-site from the C/RSP locations must be recoverable within 24 hours. See the procedure on **managing backups and media used** for the complete details.

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**. Incident management procedures meet the requirements of ISO/IEC standard 27001, clauses A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, and A.16.1.7.

The steps taken serve to minimize damage in the event of incidents. Also see the **security incident management process** and the **Apps Incident procedure** in Podio.

5.7.2 Corrupted Computing Resources, Software and/or Data (Equipment, 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.

The Business Continuity Plan is a critical component of Notarius’s management approach. The goal of managing business continuity is to identify potential threats to the organization and the impact these threats might have on operations and to provide a framework for building organizational resilience and the ability to respond efficiently.

This process is defined in the **Business Continuity Policy** document. This plan is tested at least once every two (2) years. The Vice-President of Operations and Product Strategy is responsible for activating the BCP.

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 third 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;
- Issue an updated CRL, the day after the compromise.

As an example, see **BCP—Compromised Root CA**.

5.7.4 Business Continuity Capabilities after a Disaster

The C/RSP has a Business Continuity Plan (BCP) in place to meet the availability requirements of the various functions outlined in this CPS, the CA’s commitments in this CPS, and the results of the risk analysis.

The BCP includes, among other things, the scenario of a compromised Root CA key.

The C/RSP’s BCP is composed of three distinct documents:

- **BCP—Business Continuity Plan**
-

- **BCP—Crisis Response**
- **BCP—Annex A Scenario 1-5**

5.8 Termination of Activities

Termination of activities includes either the transfer of activities to another entity or the complete termination of activities.

- **Transfer of activity** means the end of a component of the CA's activity having no effect on the validity of the certificates issued prior to the intended transfer and the resumption of said activity by the CA with a new entity. In such cases, to maintain the level of trust during and after the transfer of activity, the CA agrees to notify its customers immediately of any upcoming changes and put procedures in place to ensure consistent service.
- **Termination of activity** means the end of a component of the PKI's activity having an effect on the validity of the certificates issued prior to the intended termination. Termination may be complete or partial (e.g., termination of activity for a given group of certificates only).

5.8.1 CA Termination

To the extent possible, 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.

In case of CA end of life, the CRL issued by Notarius will be issued with a NextUpdate field value of 99991231235959Z.

This last CRL will not be issued until all certificates covered by said CRL have expired or been revoked. In the event that the PSC/R removes revoked Certificates from the CRL after they have expired, the CRL will not include the X.509 extension "ExpiredCertsOnCRL" as defined in ISO/IEC 9594-8/Recommendation ITU T X.509.

If the C/RSP decides or is required to terminate a CRL, it shall issue and publish at the corresponding CRL distribution point a final CRL with a nextUpdate field value as defined in ETSI EN 319 411-1 [2], clause 6.3.9. Requirement CSS-6.3.9-06.

The procedures for transferring operations and responsibilities shall be agreed upon between the CA and the C/RSP. The minimum duration of continued revocation status shall be two (2) years as specified in the escrow agreement.

Specifically, the CA agrees to:

- Notify its clients using the appropriate means of communication;
- Revoke all certificates issued by the CA;
- Refrain from transmitting the private keys that enabled them to issue certificates or CRLs to any person whatsoever;
- Destroy the private keys and all backup copies of the private keys that enabled it to issue certificates or CRLs.

A *specific scenario* has been documented by the C/RSP in the event of such termination in accordance with eIDAS requirements.

5.8.2 C/RSP Termination

The C/RSP will notify the CA at least three (3) months in advance of its intention to cease operations

Transfer arrangements will be discussed 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

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

Termination may have a major impact on LRA member clients, for example. To minimize the impact of such a situation, the C/RSP must ensure that the clauses of the contract are respected, that adequate communication takes place with the various stakeholders, and that the possibility of transferring LRA members to another product is evaluated.

The following procedure applies in the event of termination of LRA activities: ***LRA end-of-contract procedure***.

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

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
 - Steps are documented in the Wiki and implemented by the technical team
 - Tests are completed to validate the steps in the key ceremony process
- By individuals in pre-established trusted roles who have been approved by the C/RSP's executive committee
 - Details on the trusted roles are provided in the Wiki:
 - **Roles matrix - PKI and SS portal**
 - **Roles Matrix - HSM portion**
 - Formal **commitments** are signed by each person occupying a role.
 - Security checks are completed by the C/RSP at planned intervals and saved in the employee's **HR file**.
- As part of an official "Key Ceremony"
 - **Agenda example**
 - **Ceremony example**
 - **Example of minutes**

CA signing keys are generated during an official ceremony using a physical cryptographic resource that meets the requirements of the security level in question (FIPS 140-2).

The cryptographic devices used for CA key generation use a random number generator (RNG).

During the key ceremony, all operations are conducted under strictly controlled conditions by persons in trusted roles and in accordance with the applicable procedure.

Key ceremonies take place on C/RSP premises. They are overseen by at least two persons holding the trusted roles of Security Officer or Operations Manager and in the presence of an impartial outsider. Witnesses attest, in an objective and factual manner, to the conduct of the ceremony in relation to the previously defined script.

The ceremony is recorded in signed minutes attesting that it has been conducted in accordance with the established procedure and demonstrating that the integrity and confidentiality of the key pair generation has been ensured. Minutes are stored on the C/RSP network.

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.

The PKI application manages two distinct key pairs, one for encryption and the other for signing.

Key pairs are generated using cryptographic algorithms in accordance with the specifications expressed below and following the PKIX-CMP exchange protocol²:

- Signing keys are generated by the holder using a software or hardware cryptographic module.
- Encryption keys are generated by the CA.

6.1.1.3 Subscriber Keys Generated by Subscribers

Not applicable.

² The PKIX-CMP protocol is documented in the following IETF publications: [RFC4210](#) and [RFC6712](#).

6.1.2 Private Key Delivery to Subscribers

Keys are generated on subscribers' workstations or on a cryptographic hardware device using the C/RSP application.

A digital signature activation email that includes the first activation code is sent to the subscriber at their application email address (verified address). By activating the command provided for this purpose, the subscriber will access the "My Account" section of the C/RSP management portal. The subscriber authenticates themselves using their security questions, enters the number provided in their activation email, and selects a password that meets the CA's security standards to finalize the subscription process and generate their keys and certificates.

The certificate and public signing key are delivered following the PKIX-CMP exchange protocol.

Once delivered, the private key remains under the sole control of the holder.

The certificate including the private signature key is generated on the holder's computer according to the PKIX-CMP exchange protocol. This private key is maintained under the sole control of the holder.

The CA does not retain or copy private keys. The CA has only the public key of the generated certificate.

6.1.3 CA Public Key Delivery to Certificate Users

The CA's public signing key is made available to subscribers and third parties and is publicly available for viewing, as defined in Section 2.

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 Size

Recommendations from the competent national and international bodies (for example, relating to key lengths, signature algorithms, and hashing algorithms) are consulted annually to determine whether or not the parameters used in the issuance of CA certificates or in the issuance of holder certificates should be modified. See the ***PKI and key length and algorithms table***.

- The algorithm and key size of the root CAs, iCA1 and iCA2 is RSA-4096 bits.
- The algorithm and key size of the root CA certificate holders, iCA1 and iCA2 is RSA-2048 bits.
- The algorithm and key size of the iCA3 (server key size for a seal certificate) is type P-256 (NIST) in ECDSA.
- The algorithm and key size of iCA3 CA certificate holders can vary from ECC P-192 to P-384 (NIST) in ECDSA.

In the event that an algorithm used no longer meets the recommendations of the competent national and international organizations, the C/RSP will take measures (up to and including the revocation of certificates, if necessary) to remedy the situation within the allotted time. A communication plan will also be considered with the marketing team of the C/RSP.

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

The use of the private key seal is limited to the **Otentik VDS** 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 (Evaluation Assurance Level) 4+ ensure key protection with a security level deemed acceptable against threats to integrity, availability, and confidentiality.

QSCD equipment is validated annually by the C/RSP. Processes are put in place to replace them in case of a change in status. For example, in the event that the token sent to the holder no longer complies with the QSCD standard referred to in the ETSI EN 319 411-2 standard (SDP-6.5.1-02) for the generation of qualified certificates, the C/RSP will provide the holder with a new compliant token on which he can generate a new private key.

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

Subscribers' private keys are not escrowed.

6.2.4 Private Key Backup

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

6.2.5 Private Key Archiving

Subscribers' private keys are never archived by the CA or by any other PKI participant.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The subscriber's private key may be transferred to the cryptographic module in accordance with the requirements of Section 6.1.2.

6.2.7 Private Key Storage in the Cryptographic Module

Subscribers' private keys are protected by their cryptographic modules.

6.2.8 Multi-user Control (m of n)

The CA's private signing keys are controlled by no fewer than two (2) individuals in trusted roles in accordance with the "m of n" authentication method.

6.2.9 Protecting Subscribers' Private Keys

Subscribers are solely responsible for the protection of their private keys.

The use of the digital signature is a personal right, and, in this sense, it is strictly forbidden for the holder to entrust or disclose the information allowing its use to anyone whomsoever. Violations will result in the immediate revocation of the digital signature.

In this sense, holders must take all necessary measures to ensure the security and confidentiality of their private keys, in particular by not disclosing the passwords they have set. Passwords must respect specific criteria, which the C/RSP must make known to holders. Specifically, passwords:

- Must be at least eight (8) characters long
- Must contain at least one (1) uppercase letter
- Must contain at least one (1) lowercase letter
- Must contain at least one (1) digit
- Must not contain more than half of the full name of a security deposit
- Must not repeat the same character for in more than half of the password

Although a period of automatic inactivity can be configured for an application or workstation, holders must always verify that access to their private keys is disabled before leaving their workstations.

When a holder no longer uses their keys and certificates, they must destroy them by deleting the file so that the data may not be recovered.

Note that a copy of the private encryption keys is kept by the C/RSP in anticipation of an eventual recovery. These keys remain encrypted at all times by and within the PKI application.

6.2.10 Private Key Activation Method

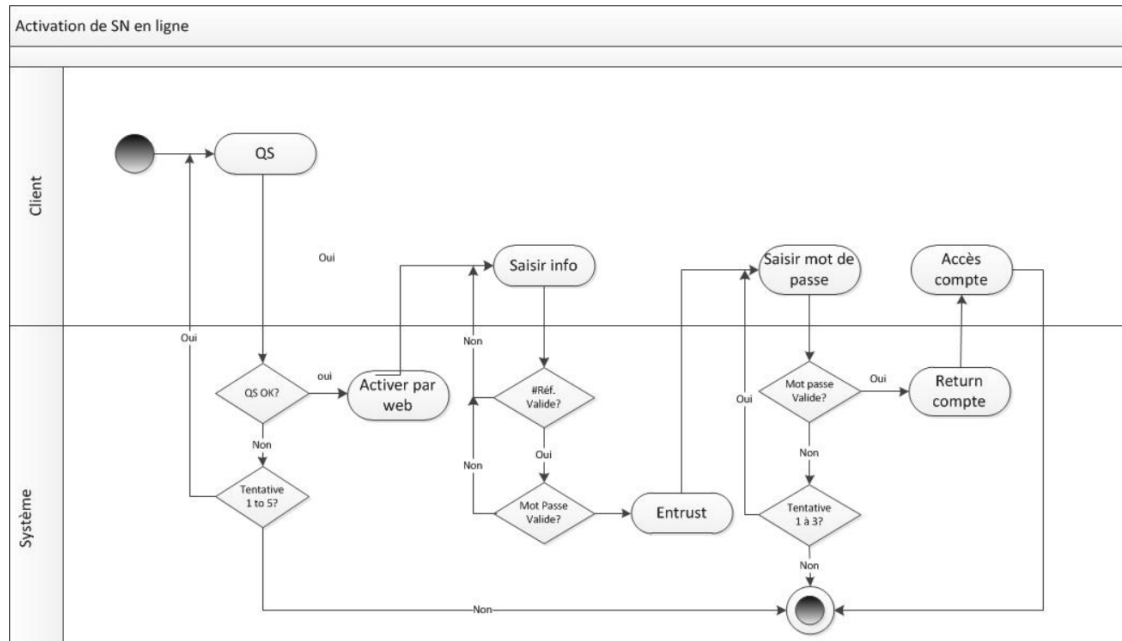
6.2.10.1 *Activating the CA's Private Key*

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

6.2.10.2 *Activating the Subscriber's Private Key*

The activation of the holder's private key is controlled via activation data.

The private key can be activated using the C/RSP management portal in the "My account" area



OR directly via EESP (Entrust Entelligence) by entering an Entrust number ID.

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

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

6.2.12.2 Destroying the Subscriber's Private Key

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

6.2.13 Evaluation of the Cryptographic Module

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

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

- Ensures the confidentiality and integrity of the CA's private signing keys throughout their

- lifetime, including destruction according to high security standards;
- Identifies and authenticates its users;
- Creates audit records.

6.3 Other Aspects of Key and Certificate Management

6.3.1 Public Key Archival

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

6.3.2 Certificate and Key Usage Periods

In principle, the operational life of a certificate ends either when it expires or is revoked. CA servers cannot issue certificates with a lifespan that exceeds the CA's own certificate. The usage periods for the keys issued are as follows:

Type	Maximum lifespan - before certificate expiration
Root CA	20 years
Issuing CA	20 years
Root CA signing key, iCA1 and iCA2	3 years
Signing key for CA iCA3	10 years
Encryption key	3 years
Test key	1 year
Timestamping service (TSA - Time Stamp Authority)	10 years
Online Certificate Status Protocol (OCSP) service	2 years

The C/RSP may decide to reduce the period of maximum validity of certain certificates, for example, for test certificates.

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, as described in Section 3.2.2.

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 as stipulated in the general terms of use for Notarius products and in specific contractual agreements, where applicable. Activation data that is generated by the CA for holders' cryptographic modules is fully protected and remains confidential until delivery to the recipient. Holders are then responsible for ensuring their confidentiality, integrity, and availability.

6.4.1 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 (for example, the **Secure Development Policy**).

Risk analyses are conducted when needed according to the documented requirements and **procedures**.

A minimum level of assurance of the security provided on the PKI component information technology infrastructure is defined in the **ITC management policy**, the **Notarius Security Policy**, and the **information security management system (ISMS) statement of applicability**.

Requirements of the eIDAS standard are also **documented and implemented**.

These reference documents, available on the C/RSP Wiki, respond in particular to 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.

The protection of the confidentiality and integrity of private infrastructure keys is subject to specific measures, arising from the **risk analysis (Class C)** and annual reviews, or when necessary.

Monitoring systems and **PKI audit** procedures are in place.

PKI configuration, as well as all modifications and developments, are documented and controlled by the C/RSP. All unauthorized modifications are detected.

Configuration management is used for the installation and subsequent maintenance of the CA system. The first time the software is loaded, we confirm that the software is the one delivered by the vendor, that it has not been modified before being installed, and that it corresponds to the desired version.

Systems development is controlled by ensuring that:

- Software and hardware are acquired in such a way as to reduce the possibility of a particular component being tampered with;
- The software developed has been developed in a controlled environment, and the development process is defined and documented;
- Hardware and software dedicated to PKI are not used for other activities;
- The software installed is scanned for malicious code before first use and periodically thereafter;
- Hardware and software updates are installed by personnel in trusted roles who have been trained according to current procedures.

The PKI management application and production networks are logically separated from the other components of the C/RSP.

This separation prevents unauthorized accesses to the production applications.

The C/RSP uses firewalls to protect production networks from internal and external intrusions and limits the nature and source of network activities that can access them.

The C/RSP requires the use of a password containing a minimum of characters and consisting of an alphanumeric combination. The password must be changed on a regular basis.

Direct access to databases or applications supporting PKI operations is limited to individuals identified in the **trusted roles matrix** to perform their functions and requires “trusted role” keys and certificates with specific rights to access them.

The CA can be accessed at controlled computer workstations.

The accessible components of the PKI are connected to the Internet in an adapted architecture with security gateways and ensure continuous service (except during maintenance or backup operations). Other PKI components use appropriate security measures to ensure that they are protected against denials of service and intrusion attacks. These measures include the use of firewalls and filtering routers.

Unused ports and network services are cut off.

All flow control devices used to protect the network on which the PKI is hosted deny all but the necessary services, even if those services have the capability to be used by other devices on the network.

The local network equipment used by the CA is maintained in a physically secure environment and its configurations are periodically reviewed.

6.6 Control Measures

Modules for key generation and cryptographic operations must comply with the specifications set out in Section 6.2.

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 according to the established **methodology**.

The C/RSP uses applications and components that have been previously verified to ensure a sufficient quality guarantee and backward compatibility and that they meet the specifications set out in Section 6.2.

It tests and documents any changes to the infrastructure according to the defined internal rules and in compliance with the manufacturer’s recommendations.

Based on the conclusions of the risk analysis, the C/RSP must verify backward compatibility with existing applications and components.

The C/RSP has established **systems monitoring mechanisms**.

During installation, and periodically after installation, the C/RSP tests the integrity of its systems. (See the results of the **quarterly security audits** or **PKI log audit**)

6.7 Network Security Controls

The CA undertakes to ensure that all networks used as part of the PKI meet the IT security objectives. 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.

Vulnerability monitoring and management is performed on a scheduled basis, including penetration testing and code review.

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 fingerprints can be accessed 24/7 directly on the Notarius website at <https://www.notarius.com/en/certification-policies-and-practice-statements>

- The main information contained in the certificates of the **Root CA and iCA1, iCA2 and iCA3 issuing CAs** is:

Base Field	Value for Root CA	Value for iCA1, iCA2 and iCA3 Issuing CAs
Digital fingerprint	<p>Notarius Root Certificate Authority ⁽¹⁾ (2014-2034): 1f 3f 14 86 b5 31 88 28 02 e8 7b 62 4d 42 02 95 a0 fc 72 1a</p> <p>Notarius Root Certificate Authority ⁽¹⁾ (2021-2036) : b1 c3 ac 09 77 aa f1 47 e5 82 1a 87 f8 da 32 22 6a 21 06 93</p>	<p>Notarius Certificate Authority ⁽²⁾ (2015-2034) - ICA1: bb 05 7f 07 4c 92 da db 5e 49 52 43 e2 59 a0 3f e1 6b d6 87</p> <p>Notarius Certificate Authority ⁽²⁾ (2021-2036) – ICA1 : 77 16 bf f6 1d 97 10 d7 7b 93 f0 7e 33 24 72 6c 5f 33 76 c5</p> <p>Notarius Certificate Authority 2 ⁽³⁾ (2015-2034) - ICA2: 7f 44 93 cb 96 11 82 3f c3 e1 2d bb 96 e1 b9 ef 93 a6 84 e3</p> <p>Notarius Certificate Authority 2 ⁽³⁾ (2021-2036) – ICA2 : c5 5a f7 c7 c3 1e 93 86 39 7f e8 f6 71 3d 0b 56 bc ef bc 8b</p> <p>Notarius Certificate Authority 3 ⁽³⁾ (2019-2034) - ICA3: c0 99 e4 55 9f f5 17 35 24 23 8e 13 4e ab 7b c3 6d 00 b8 76</p> <p>Notarius Certificate Authority 3 ⁽³⁾ (2021-2036) – ICA3 : ba 6a 66 c3 d4 d4 12 a1 2e e5 d2 27 5b c6 8e f9 b4 8d 71 d8</p>
Issuer DN	<p>cn=Notarius Root Certificate Authority o=Notarius inc c=CA</p>	<p>cn=Notarius Root Certificate Authority o=Notarius inc c=CA</p>
Subject DN	<p>cn=Notarius Root Certificate Authority o=Notarius Inc</p>	<p>cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius inc</p>

	c=CA	c=CA
Length of CA keys	4096	4096 256 for ICA3
Key pair algorithm	RSA	RSA ECDSA for ICA3
Maximum duration before certificate expiry	20 years	20 years

(1) *Notarius Root Certificate Authority = Root certificate also published by Microsoft as a trusted root in its certificate store.*

(2) *Notarius Certificate Authority = Intermediate Authority Certificate automatically recognized by Adobe and Microsoft.*

(3) *Notarius Certificate Authority 2 & 3 = Intermediate authority certificates automatically recognized by Microsoft.*

- The main information contained in a **certificate holder's certificate for root CAs, iCA1 and iCA2** is:

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	User role; Certificate policies; Key usage; Mail.

- The main information contained in a **holder's certificate for iCA3** is:

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device]

	uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	192 to 384
Certificate period of validity	6 months to 10 years
Certificate extension	Authorized use: AIGCEV User role; Certificate policies; Key usage;SubjectAltName.

▪ ***ICA1 – AATL Certificate Profile***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	Certificate policies = Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> (2.16.124.113550.2.2.1.1) Natural person / <i>Personne physique</i> (2.16.124.113550.2.2.2.1) Complies with the Adobe Approved Trust List (AATL) / <i>Conforme à Adobe Approved Trust List (AATL)</i> (2.16.124.113550.2.2.4.2) Cryptographic support required / <i>Support cryptographique requis</i> (2.16.124.113550.2.2.3.2) Esi4-qcStatement-1 (0.4.0.1862.1.1) AIA = http://ocsp1.notarius.com/ocsp1-ca1 (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique, Non-Répudiation (2.5.29.15); Extended Key Usage = URL TSA Personnalisée (1.2.840.113583.1.1.9.1) CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email

- ***iCA1 – AATL Evaluation Certificate Profile***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	Certificate policies = Identity NOT verified / <i>Identité NON vérifiée</i> (2.16.124.113550.2.2.1.0) Natural person / <i>Personne physique</i> (2.16.124.113550.2.2.2.1) Complies with the Adobe Approved Trust List (AATL) / <i>Conforme à Adobe Approved Trust List (AATL)</i> (2.16.124.113550.2.2.4.2) Intended for Adobe test / <i>Pour test Adobe</i> (1.2.840.113583.1.2.2) Cryptographic support required / <i>Support cryptographique requis</i> (2.16.124.113550.2.2.3.2) AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalisée (1.2.840.113583.1.1.9.1) CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email

- ***ICA1 - CertifiO Cloud Certificate Profile***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incrémenté d'un chiffre au besoin</i>] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA

Key length	2048
Certificate period of validity	6 mois, 1 an, 2 ans ou 3 ans
Certificate extension	<p>Certificate policies = Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.2.1.1) Natural person / Personne physique (2.16.124.113550.2.2.2.1) Conforme à Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2) QCP-n-qscd (0.4.0.194112.1.2)</p> <p>Esi4-qcStatement-1 (0.4.0.1862.1.1)</p> <p>AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1)</p> <p>Key usage = Signature numérique, Non-Répudiation (2.5.29.15); Extended Key Usage = URL TSA Personnalisée (1.2.840.113583.1.1.9.1)</p> <p>CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl</p> <p>Mail = Email</p>

▪ ***iCA1 - HSM AATL Profile***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	<p>Certificate policies = Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.2.1.1) Legal person / Personne morale (2.16.124.113550.2.2.2.2) Complies with the Adobe Approved Trust List (AATL) / Conforme à Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2)</p>

	<p>AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1)</p> <p>Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalisée (1.2.840.113583.1.1.9.1)</p> <p>CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl</p> <p>Mail = Email</p>
--	--

▪ **iCA1 - Evaluation HSM AATL Profile**

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	<p>Certificate policies = Identity NOT verified / <i>Identité NON vérifiée</i> (2.16.124.113550.2.2.1.0) Legal person / <i>Personne morale</i> (2.16.124.113550.2.2.2.2) Complies with the Adobe Approved Trust List (AATL) / <i>Conforme à Adobe Approved Trust List (AATL)</i> (2.16.124.113550.2.2.4.2) Intended for Adobe test / <i>Pour test Adobe</i> (1.2.840.113583.1.2.2) Cryptographic support required / <i>Support cryptographique requis</i> (2.16.124.113550.2.2.3.2)</p> <p>AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1)</p> <p>Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalisée (1.2.840.113583.1.1.9.1)</p> <p>CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl</p> <p>Mail = Email</p>

▪ ***iCA2 - Standard Certificate Profile***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	Certificate policies = Software support / <i>Support logiciel</i> (2.16.124.113550.2.3.3.1) Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> (2.16.124.113550.2.3.1.1) Individual's identity / <i>Identité d'un individu</i> (2.16.124.113550.2.3.2.1) AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1) Key usage = Digital signature (2.5.29.15); Extended Key Usage = Customized TSA URL (1.2.840.113583.1.1.9.1) CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl Mail = Email

▪ ***iCA2 - Standard Profiles with Encryption***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	Certificate policies = Software support / <i>Support logiciel</i> (2.16.124.113550.2.3.3.1) Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> (2.16.124.113550.2.3.1.1)

	<p>Individual's identity / <i>Identité d'un individu</i> (2.16.124.113550.2.3.2.1)</p> <p>AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1)</p> <p>Key usage = Digital signature (2.5.29.15);</p> <p>Extended Key Usage = Customized TSA URL (1.2.840.113583.1.1.9.1)</p> <p>CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl</p> <p>Mail = Email</p>
--	--

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	<p>Certificate policies =</p> <p>Software support / <i>Support logiciel</i> (2.16.124.113550.2.3.3.1)</p> <p>Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> (2.16.124.113550.2.3.1.1)</p> <p>Individual's identity / <i>Identité d'un individu</i> (2.16.124.113550.2.3.2.1)</p> <p>AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1)</p> <p>Key usage = Digital Signature (2.5.29.15);</p> <p>Extended Key Usage = Customized TSA URL (1.2.840.113583.1.1.9.1)</p> <p>CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl</p> <p>Mail = Email</p>

▪ ***iCA2- Evaluation Standard Profile***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA

Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	6 months, 1 year, 2 years or 3 years
Certificate extension	Certificate policies = Software support / <i>Support logiciel</i> (2.16.124.113550.2.3.3.1) Individual's identity / <i>Identité d'un individu</i> (2.16.124.113550.2.3.2.1) Identity NOT verified / <i>Identité NON vérifiée</i> (2.16.124.113550.2.3.1.0) Intended for Adobe test / <i>Pour test Adobe</i> (1.2.840.113583.1.2.2) AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1) Key usage = Digital signature (2.5.29.15); Extended Key Usage = Customized TSA URL (1.2.840.113583.1.1.9.1) CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl Mail = Email

- ***ICA3 - Standard Certificate Profile***

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	ECDSA 192 to 384
Certificate period of validity	6 months to 10 years
Certificate extension	Certificate policies = Identity verified face-to-face / <i>Identité vérifiée en face-à-face</i> (2.16.124.113550.2.4.1.1) Legal person / <i>Personne moral</i> (2.16.124.113550.2.4.2.2) Cryptographic support required / <i>Support cryptographique requis</i> (2.16.124.113550.2.4.3.2) Intended for server automation / <i>Pour serveur automatisé</i> (2.16.124.113550.2.4.4.1) Key usage = Digital signature (2.5.29.15); Extended Key Usage = AIGCEV Authorize-use (1.3.6.1.4.1.51528.1.1)

	<p>CPD = http://crl1.notarius.com/crl1-ca3/crl/notarius_certificate_authority_3_crlfull.crl</p> <p>SubjectAltName = URL=http://uri.aigcev.org/[unifromRessourceIdentifler]</p>
--	--

▪ **iCA3 - Evaluation Standard Profile**

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	ECDSA 192 to 384
Certificate period of validity	6 months to 10 years
Certificate extension	<p>Certificate policies = Identity NOT verified / <i>Identité NON vérifiée</i> (2.16.124.113550.2.4.1.0) Legal person / <i>Personne moral</i> (2.16.124.113550.2.4.2.2) Software support / <i>Support logiciel</i> (2.16.124.113550.2.4.3.1) Intended for server automation / <i>Pour serveur automatisé</i> (2.16.124.113550.2.4.4.1) Intended for Adobe test / <i>Pour test Adobe</i> (1.2.840.113583.1.2.2) AIGCEV test-certificate (1.3.6.1.4.1.51528.2.1)</p> <p>Key usage = Digital signature (2.5.29.15);</p> <p>Extended Key Usage = AIGCEV Authorize-use (1.3.6.1.4.1.51528.1.1)</p> <p>CPD = http://crl1.notarius.com/crl1-ca3/crl/notarius_certificate_authority_3_crlfull.crl</p> <p>SubjectAltName = URL=http://uri.aigcev.org/[unifromRessourceIdentifler]</p>

7.2 CRL Profile

CRLs comply with X.509, version 3.

If the C/RSP removes revoked certificates from the CRL after they have expired, the CRL will not include the X.509 extension "ExpiredCertsOnCRL" as defined in ISO/IEC 9594-8/Recommendation ITU T X.509.

If CRLs are provided and Notarius decides or is required to terminate a CRL, it shall issue and publish

at the corresponding CRL distribution point a final CRL with a nextUpdate field value as defined in ETSI EN 319 411-1 [2], clause 6.3.9. Requirement CSS-6.3.9-06 (CRL termination may occur when there are no more valid certificates in the scope of the CRL, e.g., when the CRL Signing Entity certificate expires or when the CRL Signing Entity private key is downgraded).

In the event of CA compromise, Notarius will broadcast a CA revocation status CRL with the updated revocation status on the distribution points already defined.

In case of CA end of life, the CRL issued by Notarius will be with a NextUpdate field value of 99991231235959Z.

Notarius will not issue a final CRL until all certificates covered by this CRL have expired or been revoked.

- http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl
- http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl

Base Field	Value
Issuer	CN = Notarius Certificate Authority O = Notarius Inc C = CA
Effective date	
Next update	
Signature algorithm	sha256RSA
Signature hashing algorithm	sha256
Certificate revocation list number	Number of CRLs =0e d0
Authority key identifier	1d 5a 27 f6 e5 ac 17 84 6b d1 04 1e 84 ec d4 2c ad 3f d3 7f

- http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl

Base Field	Value
Issuer	CN = Notarius Certificate Authority 2 O = Notarius Inc C = CA
Effective date	
Next update	
Signature algorithm	sha256RSA
Signature hashing algorithm	sha256
Certificate revocation list number	Number of CRLs =0d 4d
Authority key identifier	ef f7 25 89 43 bf ac b7 a4 13 55 b3 ee b1 74 b6 02 6a 38 4b

- http://crl1.notarius.com/crl1-ca3/crl/notarius_certificate_authority_3_crlfull.crl

Base Field	Value
Issuer	CN = Notarius Certificate Authority 3 O = Notarius Inc C = CA
Effective date	
Next update	
Signature algorithm	SHA256ECDSA
Signature hashing algorithm	sha256
Certificate revocation list number	Number of CRLs = [incremental number]
Authority key identifier	1499b78f9ad1f7bb75506ed3fd32a13a0fd43fc3

- http://crl.notarius.com/notarius_root_ca/crl/crl_roota1.crl

<i>Base Field</i>	<i>Value</i>
Issuer	CN = Notarius Root Certificate Authority O = Notarius Inc C = CA
Effective date	5 septembre 2019 10:26:30
Next update	16 décembre 2019 19:00:00
Signature algorithm	sha256RSA
Signature hashing algorithm	sha256
Certificate revocation list number	Number of CRLs =0b
Authority key identifier	Key ID=99 c9 10 4a 7d 78 ba 89 56 31 4e f5 ec 35 73 3d a4 1b ed 6e
Distribution point emission	<p>Nom du point de distribution :</p> <p>Nom complet :</p> <p>Adresse d'annuaire :</p> <p>CN=CRL1 CN=Notarius Root Certificate Authority O=Notarius Inc C=CA URL=ldap://X1- PROD/cn=CRL1,cn=Notarius%20Root%20Certificate%20Authority,o=Notarius%20Inc, c=CA? authorityRevocationList?base</p> <p>URL=http://crl.notarius.com/notarius_root_ca/crl/crl_roota1.crl</p> <p>Ne contient que des certificats utilisateur=Non</p> <p>Ne contient que des certificats d'autorité de certification=Oui</p>

	Liste de révocation des certificats indirects=Non
--	---

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 from IETF standard.

OCSP responses contain validity dates that enable users to establish whether the OCSP response is sufficiently up to date for their intended use. The OCSP responder uses the ArchiveCutOff extension as specified in IETF RFC 6960, with the archiveCutOff date set to the notBefore date and time value of the CA certificate.

- **OCSP Certificate Profile – iCA1**

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority <i>[incremented by one digit if necessary]</i> o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	10 years
Period of validity of the private key	2 years
Certificate extension	Certificate policies = Cryptographic support required / <i>Support cryptographique requis</i> (2.16.124.113550.2.2.3.2); Intended for server automation / <i>Pour serveur automatisé</i> (2.16.124.113550.2.2.4.2); Key usage = Digital signature (2.5.29.15); Extended Key Usage = OCSP Signature (1.3.6.1.5.5.7.3.9);
CRL distribution point	http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl
1.3.6.1.5.5.7.48.1.5	No Revocation Check

- **OCSP Certificate Profile– iCA2**

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority 2 [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	10 years
Period of validity of the private key	2 years
Certificate extension	Certificate policies = Cryptographic support required / <i>Support cryptographique requis</i> (2.16.124.113550.2.3.3.2); Intended for server automation / <i>Pour serveur automatisé</i> (2.16.124.113550.2.3.4.2); Key usage = Digital signature (2.5.29.15); Extended Key Usage = OCSP Signature (1.3.6.1.5.5.7.3.9);
CRL distribution point	http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl
1.3.6.1.5.5.7.48.1.5	<u>No Revocation Check</u>

- **OCSP Certificate Profile – iCA3**

n/a

7.4 TSA Profile

Base Field	Value
Issuer DN	cn=Notarius Certificate Authority [<i>incremented by one digit if necessary</i>] o=Notarius Inc c=CA
Subject DN	cn=[name of certificate holder, group or device] uid=[unique identifier] ou=[name of RPA or company] o= [product name] c=CA
Key length	2048
Certificate period of validity	10 years

Period of validity of the private key	2 years
Certificate extension	<p>Certificate policies = Complies with the Adobe Approved Trust List (AATL) / <i>Conforme à Adobe Approved Trust List</i> (AATL) (2.16.124.113550.2.2.4.2) Cryptographic support required / <i>Support cryptographique requis</i> (2.16.124.113550.2.2.3.2)</p> <p>Extended Key Usage = Tampon temporel (1.3.6.1.5.5.7.3.8)</p> <p>CPD =</p> <p>Mail = Email</p>
AIA	http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp

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 the CP, this 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

The CA is responsible for ensuring that PKI components are working properly by performing regular internal compliance checks and tests.

- Before any major PKI component is deployed, a ceremony is conducted according to a defined process. An external witness is always present, and the PKI Officer provides a detailed report.
- Important changes are all documented in *releases*.

The C/RSP may also undergo external audits at the request of LRAs with which it has entered into agreements for this purpose to ensure compliance with the SLAs, the provisions of the agreement, as well as the CPS, CP, and the internal policies referred to in these two documents.

Audits will be based on operational information and will not include any personal information. Each party will bear the cost of its own resources.

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](#)], [ISO 27001](#) and [ISO 9001](#).

8.2 Identity/Qualification of Assessor

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

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

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.

Internally, the C/RSP has established a number of procedures to be followed in order to meet these requirements:

- *Quarterly security audit*
- *PKI log audit*
- *Internal audit procedure*
- *Proc_gestion_nc_dac_dap*
- *Quality policy*
- *Security policy*

Externally, external auditors that are duly authorized to carry out these controls are named by the C/RSP or business partners and must be independent from the CA and the C/RSP. Before completing their tasks, they must sign *contractual agreements* and *confidentiality agreements*.

External auditors may not belong to the entity that operates the audited component, regardless of what the component is, and, if the CA as a whole is being audited, may not belong to the CA's operational divisions.

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. Their role is added to their **job description**.

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. They are selected in accordance with the **provider selection process** in place.

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.

Audits are planned annually. They may also be ad hoc or periodic.

During an external audit, the scope of the subjects or elements to be verified may be more precise or restricted depending on whether the audit is a control or re-certification audit.

The external auditor will establish an **audit program** before beginning that precisely defines which certification service components are to be audited.

The certification scope statement is transferred to the certificates issued by the external auditor after the audit.

8.5 Actions Taken as a Result of Deficiency

Following an external audit, the auditor must formally submit a **confidential report** to the C/RSP outlining specific deficiencies, minor deficiencies, and opportunities for improvement.

The C/RSP is responsible for resolving non-conformities immediately and proposing an appropriate timetable for the resolution of minor deviations and opportunities for improvement.

The report's conclusions are presented to the dedicated **committees**.

Non-conformities, minor deviations, and opportunities for improvement are addressed in a **dedicated space in Podio**.

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.

The certificates are available for consultation at all times on the C/RSP's website for ISO [9001](#), ISO [27001](#) and [eIDAS](#) certification.

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.

Current pricing for acquiring certificates is published on the Notarius website at [https://notarius.com/Products & Solutions](https://notarius.com/Products&Solutions).

The Executive Committee (C/RSP) approves fee updates.

Once an update is approved, the Marketing team updates the website and the CRM, if applicable, usually using Podio requests.

Before the new fees go into effect, the C/RSP agrees to notify the customers and partners who are negatively impacted at least one month in advance by informing them of the effective date of the new fees.

Specific contractual agreements can limit price increases in terms of the amount or a freeze period.

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 third parties who need to access the CRL to verify the validity of subscribers' certificates.

For this purpose, an agreement must be made first 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. In such cases, all persons affected by said fees will be notified.

The C/RSP may also charge fees for:

- Certificate renewal requests;
- Key and certificate renewals;
- Certificate revocations.

9.1.5 Refund Policy

In compliance with the general terms and conditions of use, Notarius will only reimburse the buyer for subscription fees that meet the following requirements: (i) in the event that an RPA or an employer refuses an application for subscription to one or more products; or (ii) if the holder is unable to install the applications required to activate their digital signature.

All other fees and payments are non-refundable, non-cancellable and non-creditable during the subscription period, including in particular in the event that the holder is no longer a member of the RPA.

9.2 Financial Responsibility

The CP sets no limitations on the value of transactions for which certificates may be used. However, certain contractual agreements 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 and adapted to information technologies.

Contracts are filed in a dedicated directory by the C/RSP.

Additionally, a copy of the proof of insurance, including the limitations of liability for the insurance amounts, may be sent by request in writing to the manager listed in Section [1.8.2](#) of this document.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for User Entities

Not applicable.

9.3 Confidentiality of Professional 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 by the LRA;
- Technical information relating to the operational security of certain components of the PKI and its infrastructure.

The C/RSP, LRAs, IVAs, and AVAs take necessary steps to protect the confidential information in their possession.

This confidential information is only used and communicated externally:

- When providing the certification services defined in this document;
- When so required by law;
- When performing work or providing certification services that have been entrusted to a service provider authorized by the C/RSP;
- When terminating the activities of the C/RSP. At such time, the C/RSP must obtain a personal data transfer agreement during the notice period.

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 concerns 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 respect, 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

Notarius Solutions Inc. holds all intellectual property rights over the CP, CPS, and PKI applications and technological infrastructure.

The cabinets where the technological infrastructure is stored at the production and backup site are leased to specialized companies in the field that meet stringent security criteria (see colocation agreements).

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 CPS is strictly prohibited, including but not limited to electronic, mechanical, optical, photocopying, and computer recording.

The terms Notarius® and CertifiO® are registered trademarks of Solutions Notarius 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

The C/RSP ensures that the mandatory information contained in certificates requiring a subscription accurately reflects the information that is verified and confirmed by the IVA and/or AVA, depending on procedure required for the trust level of the product/type of certificate.

9.6.2 Regarding Information in the Repository

The C/RSP must ensure that the CRLs published in the directory are accurate.

9.7 Limitations of Warranties

The limitations of warranties are stipulated in the general and specials terms of use of Notarius products in the section [Limitation of warranty and liability](#).

9.8 Limitations of Liability

Unless otherwise stipulated in a specific contractual agreement, the [limitations of liability](#) are described in the general conditions of use of Notarius products available.

Subject to applicable provisions of public order, the CA and the C/RSP may not be held responsible for unauthorized or non-compliant use of certificates, their associated private keys and activation data, CRLs, ARLs, or any other hardware or software made available to certificate holders.

The C/RSP accepts no liability for damage resulting from:

- Errors or inaccuracies resulting from information from the third party that completed the verification that affect the information contained in the certificates;
- The use of keys and certificates for any purpose other than those provided in the CP or expressly stated in the subscription agreement;
- The use of a revoked or expired certificate;
- Certificates marked as “test certificates” or bearing any other similar indication that such certificates cannot be reliably trusted;
- Failure to revoke a certificate that results in the use of the certificate by an unauthorized party;
- Force majeure.

Certificate holders must comply with the requirements of the CP, this CPS and the terms and conditions of the products they have purchased.

9.9 Indemnification

Unless otherwise stipulated in a specific contractual agreement, the cases of indemnification are expressed in the general conditions of use of Notarius products (see the [general terms of use](#)).

9.10 Approval Procedures

9.10.1 CP Approval Procedure

When the CP is amended, it must be submitted to the President for approval.

The CA will notify the C/RSP of any amendments that lead to changes to the CPS and, if procedures are affected, will grant a reasonable period for the C/RSP to comply with the new procedures.

Once these changes have been approved, the CP is published on the CA’s website in a timely manner.

9.10.2 CPS Approval Procedure

The CPS respects the CP.

When amendments are made to the CPS, they must be approved by the C/RSP’s Management Committee, and the CA must be notified.

9.10.3 Term of Validity

This CPS 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, new versions of the CP and CPS do not require the revocation of certificates already issued.

9.11 Individual Notices and Communications with Participants

In case of major changes to the PKI’s components, the C/RSP’s Information Security Manager will analyze the impact of such changes in terms of the security and quality of the services offered by opening and completing a risk analysis.

The **risk management procedure** is defined by the C/RSP. Risk analyses are logged and recorded in **Podio**.

9.12 Amendments

The C/RSP ensures that all changes made to the CPS remain in compliance with the laws, regulations and certification requirements.

All new versions of the CPS will be available on the CA's website.

9.13 Dispute Resolution Provisions

Customer complaints may be sent directly to Notarius customer service by chat, email, or phone (see the [Contact Us](#) page on the Notarius website). Complaints are recorded in the CRM, investigated, evaluated, and handled according to the ***complaint management procedure***.

In the event of an item of contention or dispute arising from the breach of the contractual obligations between the C/RSP and the LRA, both parties shall notify the department responsible for receiving such notices identified in the agreement in dispute by email. The date of receipt of notice shall be presumed to be the day after the date on which the email was sent.

The resolution of disputes is detailed in the [general conditions of use](#) of Notarius products.

Unless otherwise stipulated in a specific contractual agreement, an initial attempt must be made to resolve any dispute arising from the PKI services through good faith negotiations.

The aggrieved party shall notify the other party, and the members of the parties' general management teams shall first meet in good faith within fifteen (15) days from the date the dispute arose by videoconference or in a mutually agreed upon location to resolve the dispute. If the parties are unable to resolve the dispute within fifteen (15) days, they may send the dispute for mediation by following the process described below. All negotiations are confidential and must be treated as compromise and settlement negotiations for the purposes of applicable rules of evidence.

If the conflict is not resolved through good faith negotiations between the parties 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, to which the parties must abide. Either party to the dispute may notify the other party that it wishes to resolve a particular dispute through mediation. The mediator shall be appointed by mutual agreement between the parties or, if the parties are unable to reach an agreement within five (5) days after receipt of the notice of intent to mediate, the Canadian Commercial Arbitration Centre shall appoint a mediator. Mediation shall be conducted in Montreal. The language of mediation shall be that of the contract (agreement, account opening form) in dispute. The cost of mediation shall be shared equally by the parties. Any mediation rules set by the parties must be documented in writing. If the dispute is not resolved within thirty (30) days after the notice of intent to mediate, either party may terminate mediation and proceed with arbitration as set out below. All negotiations are confidential and must be treated as compromise and settlement negotiations for the purposes of applicable rules of evidence.

Subject to the provisions regarding negotiation and mediation set out above, any dispute which arises in the course of or following the performance of the present contract will be definitively settled under the auspices of The Canadian Commercial Arbitration Centre, by means of arbitration and to the exclusion of courts of law, in accordance with its General Commercial Arbitration Rules in force at the time this contract is signed and to which the parties declare they have adhered. Either party may serve notice of its intent to submit a dispute for arbitration. Arbitration shall be conducted by a single arbitrator. Arbitration shall be conducted in Montreal. The language of arbitration shall be that of the contract in dispute. The arbitrator shall not act as an amiable compositeur. The arbitrator's decision shall be final and binding for all parties and may not be appealed. The judgement on the award rendered by the arbitrator may be entered in any court of law having jurisdiction thereof. The cost of

arbitration shall be shared equally by all parties or as otherwise decided by the arbitrator. All arbitration conducted in accordance with this paragraph shall be private and confidential. The issues submitted to arbitration, hearings, proceedings, and arbitral award are strictly confidential and shall be treated as such by the parties.

For the sake of clarity, nothing contained herein shall prevent a party from seeking injunctive relief if the party believes that, without such relief, it may suffer serious harm.

The application of the UN Convention on Contracts for the International Sale of Goods is expressly excluded.

9.14 Governing Law

This CPS 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 the laws' provisions.

9.15 Interpretation

9.15.1 Applicable Laws

Applicable laws and regulations include:

- *Act to establish a legal framework for information technology*
- *Act respecting the protection of personal information in the private sector*
- *Civil Code of Québec* (SRQ, 1991, c 64), specifically Sections 36 and 37 concerning privacy and the communication of confidential information
- *Criminal Code of Canada* (RSC, 1985, c. C-46), specifically Sections 342.1, 366 and 430 concerning the interception of fraudulent information, document falsification, and mischievous behaviour, respectively
- *Copyright Act* (RSC, 1985, c C-42)
- *Trademarks Act* (RSC, 1985, c T-13)
- *Act to establish a legal framework for information technology* (CQLR, c C-1.1)
- *Quebec's Charter of Human Rights and Freedoms* (CQLR, c. C-12) and the *Canadian Constitution Act* (Schedule B to the *Canada Act 1982*, 1982, c. 11 (UK)
- *Act respecting Access to documents held by public bodies and the Protection of personal information* (CQLR, c. A-2.1)
- *Act respecting the protection of personal information in the private sector* (CQLR, c. P-39.1)
- *Personal Information Protection and Electronic Documents Act* (SC, 2005, c. 5)
- *Archives Act* (CQLR, c. A-21.1), with respect to requirements for the protection and preservation of records of heritage or archival value
- *Professional Code* (CQLR, c. C-26)

9.15.2 Validity of Provisions

The fact that one or more provisions of the CPS may be declared invalid, illegal, or unenforceable in no way affects the validity of the other provisions.

This CPS will therefore continue to apply in the absence of the unenforceable provision while respecting the intent of the parties involved.

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 CPS will be reviewed and republished annually to reflect revisions to the CP or Notarius' internal processes. A new date and version number will be applied.

9.18 Effective Date

This CPS comes into force on the date of its adoption by the Management Committee of Solutions Notarius Inc.