



Diffusion publique

POLITIQUE DE CERTIFICATION

CENTRE DE CERTIFICATION DU QUÉBEC (CCQ)

Version : 5.0

OID : 2.16.124.113550.1

Date d'approbation : 2018-12-04

Suivi des versions

Version	Date	Description	Rédacteurs	Approbateur
2.0	2001-07-16		Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
3.0	2003-04-03	Changement du nom légal de l'ICP désormais Centre de certification du Québec	Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
3.2	2005-08-26	Modification du délai de conservation des données à 10 ans & ajout d'une clause transitoire	Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
3.3	2006-05-18	Permettre des services de certification aux professionnels hors Québec	Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
3.4	2006-08-17	Suppression de la notion de certificat de base pour les notaires ainsi que de la notion de faune et parc	Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
3.5	2007-06-20	Révision pour rencontrer les exigences de la norme ISO 27001	Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
3.6	2008-02-15	Ajustement pour conformité à la norme ISO 27001	Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
4.0	2011-04-07		Liette Boulay, Directrice Services juridiques	Chambre des Notaires du Québec
4.5	2015-07-16	Décision du CE de la CNQ du 14 novembre 2012 : L'Autorité de certification est désormais le CA de Notarius TSIN inc Le PSC/R est Solutions Notarius Inc.	Liette Boulay, Directrice Services juridiques et conformité	CA de Notarius TSIN inc.
5.0	2018-04-27	Refonte complète pour conformité à la norme eIDAS	Maud Souldard, Officier ICP du CCQ Alexandre Provost, Chef d'équipe TI	CA de Notarius TSIN inc.

Propriété intellectuelle

Cette Politique de certification est la propriété exclusive de Solutions Notarius inc. Toute reproduction, impression ou transmission du présent document est strictement interdite. Pour toute reproduction intégrale ou partielle obtenir au préalable la permission écrite de Solutions Notarius Inc.

© 2018 Solutions Notarius inc.

Table des matières

1	Dispositions générales.....	7
1.1	Présentation générale.....	7
1.2	Identification du document (OID).....	8
1.3	Définition et abréviations	9
1.3.1	Abréviations	9
1.3.2	Définitions	10
1.4	Interprétation.....	12
1.5	Conformité aux normes applicables	12
1.6	Les composantes de l'ICP du CCQ.....	13
1.6.1	L'autorité de certification (AC)	13
1.6.2	Le prestataire de service de certification et de répertoires (PSC/R).....	13
1.6.3	L'autorité locale d'enregistrement (ALE)	14
1.6.4	Le détenteur.....	15
1.6.5	Autres participants	15
1.7	Utilisation des clés et des certificats.....	16
1.7.1	Utilisation autorisée des clés et des certificats	16
1.7.2	Limite d'utilisation	17
1.7.3	Détenteur autorisé	17
1.8	Gestion de la CP.....	18
1.8.1	Responsable de la CP	18
1.8.2	Coordonnées du responsable	18
1.8.3	Conformité de la CP et de la CPS	18
2	Publication et diffusion de l'information	19
2.1	Entités chargées de la mise à disposition des informations.....	19
2.2	Informations publiées.....	19
2.3	Délai et fréquence des publications.....	19
2.4	Contrôle d'accès aux informations publiées.....	20
3	Identification et authentification	21
3.1	Identification.....	21
3.1.1	Type de nom.....	21
3.1.2	Noms explicites.....	21
3.1.3	Anonymisation ou utilisation de pseudonyme	21
3.1.4	Règles d'interprétation des différentes formes de noms.....	21
3.1.5	Unicité des noms	22
3.1.6	Identification, authentification et rôle des marques déposées.....	22
3.2	Validation de l'identité.....	22
3.2.1	La vérification initiale de l'identité	23
3.2.2	La vérification de l'identité lors de la remise des données d'activation.....	24
3.2.3	La vérification de l'identité lors du renouvellement d'un certificat	24
3.2.4	La vérification de l'identité lors d'une réémission	24
3.2.5	La vérification d'identité lors d'une modification	25
4	Gestion des clés et des certificats	26
4.1	Demande d'émission de clés et de certificats	26
4.1.1	Personnes autorisées	26
4.1.2	Procédure d'adhésion.....	26
4.1.3	Approbation ou refus de la demande	26
4.1.4	Durée de validité d'une demande.....	27
4.1.5	Approbation d'un certificat	27
4.2	Demande de renouvellement d'un certificat	27
4.2.1	Personnes autorisées	27

4.2.2	Procédure de demande de renouvellement d'un certificat.....	27
4.2.3	Traitement d'une demande de renouvellement d'un certificat.....	27
4.2.4	Avis de renouvellement	28
4.3	Récupération d'un certificat	28
4.3.1	Personnes autorisées	28
4.3.2	Procédure de récupération	28
4.3.3	Traitement d'une demande de récupération.....	28
4.4	Demande de modification d'un certificat.....	28
4.4.1	Personnes autorisées	28
4.4.2	Circonstances pouvant entraîner une modification	29
4.4.3	Traitement d'une demande de modification	29
4.4.4	Avis de modification.....	29
4.5	Révocation d'un certificat	29
4.5.1	Causes possibles d'une révocation	29
4.5.2	Origine d'une demande de révocation.....	30
4.5.3	Personnes autorisées à révoquer les certificats des détenteurs.....	30
4.5.4	Traitement d'une demande de révocation	31
4.5.5	Avis de révocation	31
4.6	Suspension d'un certificat.....	31
5	Mesures de sécurité physique et opérationnelle	32
5.1	Mesures de sécurité physique.....	32
5.1.1	Situation géographique des sites	32
5.1.2	Accès physique.....	32
5.1.3	Alimentation électrique et climatisation	33
5.1.4	Vulnérabilité aux dégâts d'eau	33
5.1.5	Prévention et protection contre les incendies.....	33
5.1.6	Conservation et protection des supports	33
5.1.7	Mise hors service des supports	33
5.1.8	Prise de copie	33
5.1.9	Relève.....	33
5.2	Mesures de sécurité opérationnelle.....	34
5.2.1	Rôles de confiance	34
5.2.2	Nombre de personnes requises par tâche	34
5.2.3	Identification et authentification pour chaque rôle	35
5.2.4	Rôles exigeant une séparation des attributions	35
5.2.5	Analyse de risque	35
5.3	Mesures de sécurité relatives au personnel.....	35
5.3.1	Qualifications, compétences et habilitations requises.....	35
5.3.2	Vérifications des antécédents.....	35
5.3.3	Formation initiale	36
5.3.4	Exigences en matière de formation continue et fréquences des formations.....	36
5.3.5	Fréquence et séquence de rotations entre différentes attributions	36
5.3.6	Mesures disciplinaires	36
5.3.7	Exigences vis-à-vis du personnel des prestataires externes	36
5.3.8	Documentation fournie au personnel.....	36
5.4	Procédure de journalisation (Registre des vérifications).....	36
5.4.1	Type d'évènement enregistré	36
5.4.2	Fréquence des vérifications des registres	37
5.4.3	Conservation des registres des vérifications	37
5.4.4	Mesures de protection	38
5.4.5	Évaluation des vulnérabilités	38
5.5	Conservation et archivage des données	38
5.5.1	Types de données à conserver et archiver	38
5.5.2	Périodes de conservation des archives.....	38

5.5.3	Protection des archives	38
5.5.4	Exigence d'horodatage des données	39
5.5.5	Système de collecte des archives	39
5.5.6	Procédure de récupération et de vérification des archives	39
5.6	Changement de clés d'AC	39
5.7	Reprise par suite d'une compromission ou d'un sinistre	39
5.7.1	Procédure de remontée et de traitement des incidents et des compromissions... ..	39
5.7.2	Procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)	39
5.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante 40	40
5.7.4	Capacités de continuité d'activité suite à un sinistre	40
5.8	Cessation des activités	40
5.8.1	Cessation des activités de l'AC	40
5.8.2	Cessation des activités du PSC/R	40
5.8.3	Cessation des activités de l'ALE	40
5.8.4	Fin de vie de l'Infrastructure de gestion des clés	40
6	Mesures de sécurité techniques	41
6.1	Génération et livraison des clés	41
6.1.1	Génération des clés	41
6.1.2	Transmission de la clé privée à son propriétaire	41
6.1.3	Transmission de la clé publique de l'AC aux utilisateurs de certificats	41
6.1.4	Taille des clés	41
6.1.5	Vérification de la génération des paramètres des clés et de leur qualité	41
6.1.6	Objectifs d'usage de la clé	42
6.2	Normes de sécurité relatives aux modules cryptographiques et protection des clés privées 42	42
6.2.1	Normes de sécurité relatives aux modules cryptographiques	42
6.2.2	Protection des clés privées de l'AC (contrôle des clés privées de l'AC par plusieurs personnes)	42
6.2.3	Séquestre de la clé privée	42
6.2.4	Copie de secours de la clé privée	42
6.2.5	Archivage de la clé privée	42
6.2.6	Transfert de la clé privée vers / depuis le module cryptographique	42
6.2.7	Stockage de la clé privée dans le module cryptographique	43
6.2.8	Contrôle multi-usager (m de n)	43
6.2.9	Protection des clés privées du détenteur	43
6.2.10	Méthode d'activation de la clé privée	43
6.2.11	Méthode de désactivation de la clé privée	43
6.2.12	Méthode de destruction des clés privées	43
6.3	Autres aspects relatifs à la gestion des clés et des certificats	44
6.3.1	Archivage des clés publiques	44
6.3.2	Durées de vie des clés et des certificats	44
6.4	Données d'activation	44
6.4.1	Génération et installation des données d'activation	44
6.4.2	Protection des données d'activation	44
6.5	Mesures de sécurité informatiques	44
6.6	Mesures de contrôle	45
6.7	Mesures de sécurité réseau	45
6.8	Horodatage et système de datation	45
7	Profils des certificats, de l'OCSP, du TSA et des LCR	47
7.1	Profil des certificats	47
7.2	Profil des LCR	53
7.3	Profil OCSP	53

7.4	Profil TSA.....	54
8	Audit de conformité et autres évaluations.....	55
8.1	Fréquence et/ou circonstances des évaluations	55
8.2	Identités/Qualification des évaluateurs.....	55
8.3	Relations entre évaluateurs et entités évaluées.....	55
8.4	Sujets couverts par les évaluations	55
8.5	Actions prises suite aux conclusions des évaluations.....	55
8.6	Communications des résultats	56
9	Autres problématiques métiers et légales.....	57
9.1	Tarifs.....	57
9.1.1	Frais d'abonnement ou d'utilisation	57
9.1.2	Frais d'accès aux LCR et à l'état des certificats.....	57
9.1.3	Frais pour la vérification de l'identité	57
9.1.4	Tarifs pour d'autres services	57
9.1.5	Politique de remboursement.....	57
9.2	Responsabilité financière	57
9.2.1	Couverture par les assurances.....	57
9.2.2	Autres ressources.....	57
9.2.3	Couverture et garantie concernant les entités utilisatrices.....	57
9.3	Confidentialité des données professionnelles	57
9.3.1	Périmètre des informations confidentielles.....	57
9.3.2	Informations hors du périmètre des informations confidentielles	58
9.3.3	Responsabilités en termes de protection des informations confidentielles.....	58
9.4	Protection des données personnelles	58
9.4.1	Politique de protection des données personnelles.....	58
9.4.2	Informations à caractère personnel	58
9.4.3	Informations à caractère non personnel.....	58
9.4.4	Responsabilité en termes de protection des données personnelles.....	58
9.4.5	Notification et consentement d'utilisation des données personnelles	59
9.4.6	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives	59
9.4.7	Autres circonstances de divulgation d'informations personnelles.....	59
9.5	Propriété intellectuelle	59
9.6	Interprétations contractuelles et garanties.....	59
9.6.1	Relativement aux renseignements inscrits au certificat	59
9.6.2	Relativement aux renseignements inscrits au répertoire	59
9.7	Limite de garantie	59
9.8	Limite de responsabilité.....	60
9.9	Indemnisation	60
9.10	Procédures d'approbation	60
9.10.1	Approbation de la CP.....	60
9.10.2	Approbation de la CPS	60
9.10.3	Durée de validité.....	60
9.10.4	Applicabilité en cas d'invalidité	60
9.11	Dispositions concernant la résolution des conflits.....	60
9.12	Juridictions compétentes	60
9.13	Interprétation.....	61
9.13.1	Lois et règlements applicables	61
9.13.2	Indépendance des dispositions	61
9.14	Revue	61
9.15	Entrée en vigueur	61

1 Dispositions générales

1.1 Présentation générale

Solutions Notarius Inc. (ci-après identifié **Notarius**) a pour mission d'offrir des solutions de signatures numériques et électroniques assurant la fiabilité à long terme des documents. Elle est également prestataire de service de certification depuis plusieurs années auprès des professionnels et de leurs partenaires d'affaires.

En place depuis 1998, l'infrastructure à clés publiques (ICP) portant le nom de Centre de certification du Québec (CCQ) prévoit l'émission de clés et de certificats à des détenteurs autorisés permettant de signer et pour la clientèle notariale de chiffrer des documents électroniques.

On peut donc dire que :

- La signature numérique du CCQ certifie le statut professionnel du signataire ou son lien d'emploi;
- L'intégrité de la signature numérique protège le contenu des documents contre toute modification non autorisée.

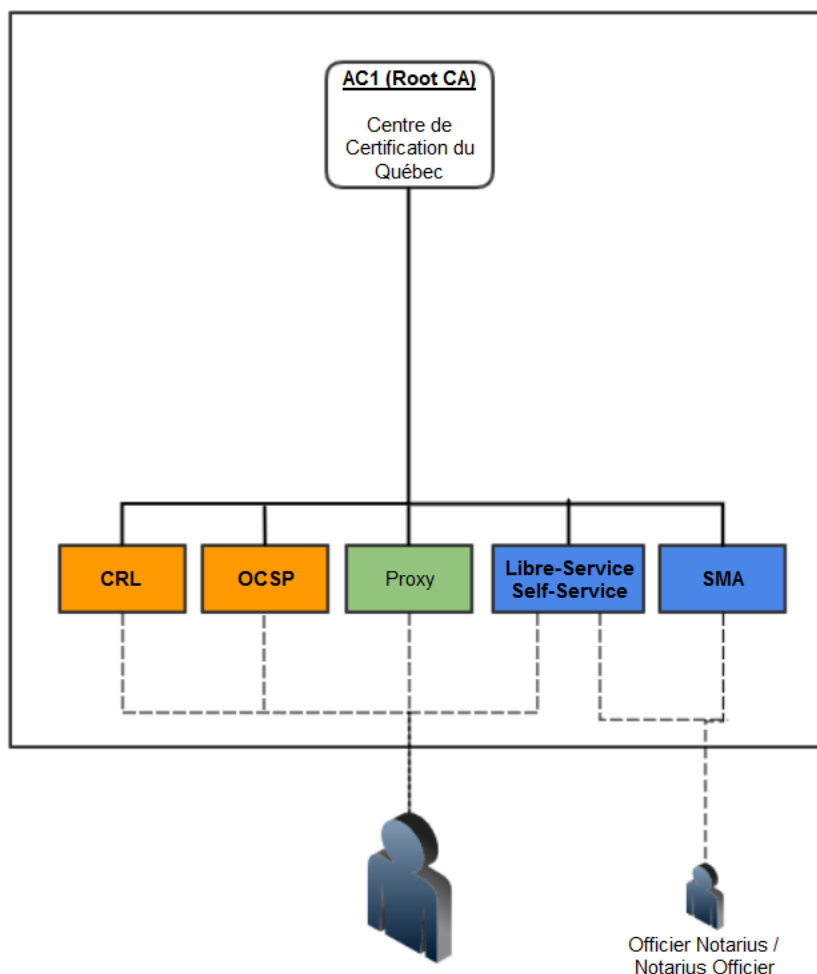
Le présent document vise donc à répondre également aux besoins de cette clientèle.

La présente Politique de Certification (ci-après identifié **CP**) définit les engagements de Notarius dans le cadre de la fourniture de certificats avancés. Cette CP est conforme aux principes et recommandations définis dans les normes ETSI EN 319 411-1 & ETSI EN 319 411-2.

Les certificats émis par le CCQ sont utilisés pour des signatures numériques ayant des effets juridiques identiques à des signatures manuscrites et qui sont par conséquent recevables en preuve sous réserve de leur confidentialité ou de toute protection conférée par le secret professionnel. Ces certificats attestent de l'identité des personnes physiques auxquelles ils ont été délivrés lorsque celles-ci agissent en tant que signataires.

Notarius délivre des certificats aux membres de son personnel ainsi qu'à ses clients, entreprises, organisations, ordres professionnels, etc.

Le périmètre de la CP du CCQ se limite au schéma ci-dessous présenté :



1.2 Identification du document (OID)

La présente CP est dénommée *Politique de certification – Centre de certification du Québec (CCQ)*. Elle est identifiée notamment par son numéro d'identifiant d'objet (OID) suivant : 2.16.124.113550.1

La CP est complétée par une *Déclaration des Pratiques de Certification (CPS)* correspondante référencée par un numéro d'OID, 2.16.124.113550.1

La Politique de certification et la Déclaration des Pratiques de Certification identifiées ci-dessus sont désignées dans la suite du document respectivement sous le nom « CP » et « CPS ».

Les identificateurs d'objet (OID) pour l'ICP du CCQ de Notarius est :

- (2) pays
- (16) Canada
- (124) Notarius
- (113550.1) Certificate Authority.
-

Notarius organise ses arcs d'OID pour les différents certificats comme suit :

Description	Identificateur d'objet (OID)
Certificat de l'AC Racine : <i>Centre de certification du Québec</i>	2.16.124.113550.1.1
• Certificat détenteur - Test	
○ Signature	2.16.124.113550.1.1.0
○ Chiffrement	2.16.124.113550.1.1.9
• Certificat détenteur - Moyen	
○ Signature	2.16.124.113550.1.1.2
○ Chiffrement	2.16.124.113550.1.1.5
• Certificat détenteur – Moyen-Élevé	
○ Signature	2.16.124.113550.1.1.3
○ Chiffrement	2.16.124.113550.1.1.6
• Certificat détenteur – Élevé	
○ Signature	2.16.124.113550.1.1.7
○ Chiffrement	2.16.124.113550.1.1.8
• Autres Fonctions	
○ Cryptographic support required / Support cryptographique requis	2.16.124.113550.1.3.2
○ Intended for server automation / Pour serveur automatisé	2.16.124.113550.1.4.2

1.3 Définition et abréviations

1.3.1 Abréviations

Les abréviations utilisées dans la CP sont les suivantes :

- AC : Autorité de certification
- ALE : Autorité locale d'enregistrement
- AVA : Agent de vérification de l'affiliation
- AVI : Agent de vérification de l'identité
- CCQ : Centre de certification du Québec
- CN : Nom commun (*Common Name*)
- CRM : Gestion de la relation client (*customer relationship management*)
- CP : Politique de certification
- CPS : Déclaration des pratiques de certification

- DN : Nom distinctif (*Distinguished name*)
- ETSI : Institut européen des normes de télécommunication (*European Telecommunications Standards Institute*)
- ICP: Infrastructure à clés publiques
- ISO : International Standard Organization
- LAR : Liste des autorités révoquées
- LCR : Liste des certificats révoqués
- LS : Libre-service
- OID : Numéro d'identifiant d'objet
- OCSP: Online Certificate Status Protocol
- PSC/R : Prestataire de services de certification et de répertoires
- RPR : Regroupement de professionnels reconnu
- RSI : Responsable de la sécurité de l'information

1.3.2 Définitions

Les termes utilisés dans la CP sont les suivants :

- **Activation** : Opération effectuée par le détenteur qui consiste à inscrire ses données d'activation dans un dispositif cryptographique pour générer ses certificats.
- **Annulation** : Intervention effectuée par le PSC/R consistant à retirer une demande d'attribution de certificats avant son activation à la demande du détenteur ou lorsque les délais prescrits d'activation ne sont pas respectés.
- **Attribution** : Émission des clés et des certificats à un demandeur.
- **Audit** : L'audit est une activité de contrôle indépendant des enregistrements et activités d'un système réalisée par un agent compétent et impartial afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures.
L'audit permet de faire le point sur le processus de gestion mis en place par le PSC/R ou ALE afin d'en dégager les points faibles ou les non-conformités. Les résultats des contrôles permettront alors au PSC/R ou l'ALE de poser les actions adéquates pour corriger les écarts et dysfonctionnements constatés.
- **Autorité de certification (AC)** : Entité responsable des certificats signés en son nom ainsi que de l'ensemble de l'ICP du CCQ. Elle peut déléguer ses fonctions à une personne qu'elle désigne.
- **Autorité locale d'enregistrement (ALE)** : Regroupement de professionnels reconnus (RPR) ou une Personne morale responsable des fonctions qui lui sont déléguées par le PSC/R. Une ALE doit avoir une entente écrite avec le PSC/R.
- **Authentification** : Processus permettant de vérifier l'identité déclarée d'un détenteur (individu, organisations) afin d'autoriser l'accès à ce détenteur à des ressources (systèmes, réseaux, applications).
- **Application client** : L'application ou le logiciel utilisé par le détenteur, installé sur un poste ou accessible en ligne, qui permet d'activer ou de récupérer ses certificats, de modifier son mot de passe, d'effectuer certaines opérations de configuration ou de réaliser des transactions au moyen de ses certificats.
- **Bi clé** : Une bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

- **Certificats** : Ensemble d'informations comprenant au minimum ce qui est prévu par la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ c C-1.1) et signé par l'AC dans le but, notamment de confirmer l'identité du détenteur.
- **Clé privée** : Clé de la bi clé asymétrique d'un détenteur qui doit être uniquement utilisée par ce détenteur.
- **Clé publique** : Clé de la bi clé asymétrique d'une entité qui peut être rendue publique.
- **Compromission** : violation avérée ou soupçonnée d'une politique de sécurité au cours de laquelle la divulgation non autorisée ou la perte de contrôle d'informations sensibles a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée ou d'autres compromissions à cette clé privée.
- **Confidentialité** : propriété qu'a une information de n'être rendue disponible ou divulguée qu'aux individus, entités ou processus autorisés.
- **CRM (Customer Relationship Management)** : Outil de gestion du PSC/R destiné à capter, traiter et analyser les informations relatives à ses clients, partenaires, employés ou prospects.
- **Détenteur de clés et de certificats** : Organisme, personne morale ou physique ayant adhéré au service et détenant des clés et des certificats de l'ICP du CCQ lui permettant de signer, s'authentifier et/ou chiffrer selon ses besoins ou les fonctionnalités disponibles. Un détenteur peut être titulaire d'un certificat qui sera affecté à un groupe, un dispositif ou une application.
- **Déclaration des pratiques de certification (CPS)** : Document qui identifie et référence les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que le PSC/R applique dans le cadre de la fourniture de ses services de certification aux usagers, et ce, en conformité avec la CP qu'il s'est engagé à respecter.
- **Demande de certificat** : message transmis par une entité pour obtenir l'émission d'un certificat de l'AC.
- **Dispositif** : application autorisée par le PSC/R permettant d'effectuer, en tout ou en partie, la gestion des clés et les certificats d'un détenteur, notamment leur activation, leur renouvellement, leur récupération, etc. Il peut s'agir d'un logiciel, d'une plateforme transactionnelle ou d'un service Web.
- **Données d'activation** : Informations nécessaires pour procéder à l'activation des clés et des certificats que le détenteur doit protéger pour en assurer la confidentialité (par ex par un PIN).
- **Émission** : Attribution de clés et de certificats à un demandeur.
- **Identifiant d'objet de politique (OID)** : Désignation numérique se retrouvant dans le certificat et faisant référence à la CP permettant d'identifier le niveau de confiance du certificat.
- **Infrastructure à clés publiques (ICP)** : Ensemble de composants physiques, de fonctions et procédures, de logiciels et de ressources humaines dédiées à la gestion des clés et certificats émis par l'AC.
- **Intégrité** : fait référence à l'exactitude de l'information, de la source de l'information et au fonctionnement du système qui la traite.
- **Libre-service (LS)** : Plateforme de gestion des signatures numériques de Notarius.
- **Liste des certificats révoqués (LCR)** : Liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus dignes de confiance (révoqués ou invalidés). Cette liste est signée par l'AC pour en empêcher toute modification par une

personne non autorisée. Elle comprend une date d'émission, une date de mise à jour (toutes 2 optionnelles) et la liste proprement dite sous la forme de paire (numéro de série du certificat révoqué ; motif éventuel de révocation).

- **Modification** : Intervention effectuée dans le but de rectifier les informations contenues dans un certificat par l'attribution d'un nouveau certificat modifié.
- **Partenaire d'affaires** : Personne morale qui désire transiger de façon électronique avec des détenteurs de certificats. Il doit être autorisé et avoir conclu une entente à cet effet avec le PSC/R
- **Personne morale** : Inclus une corporation, une société, un ministère ou un organisme public et, par extension, une société de personnes, une association et une fiducie. Le terme *Personne morale* est utilisé dans le but d'alléger le texte.
- **Politique de certification (CP)** : ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations.
- **Prestataire de services de certificats et de répertoires (PSC/R)** : Entité responsable de l'administration des services de certification et de répertoire visant la délivrance et la gestion des certificats.
- **Réattribution** : nouvelle attribution à un même détenteur à la suite d'une révocation ou d'un non-renouvellement de ses certificats.
- **Récupération** : Intervention effectuée à la demande du détenteur ou du PSC/R visant à régénérer les clés et les certificats du détenteur lorsque ceux-ci ne peuvent plus être utilisés, notamment à la suite d'un problème technique, de la destruction accidentelle de son profil ou de l'oubli de son mot de passe.
- **Regroupement de professionnels reconnus (RPR)** : Groupement professionnel, ayant une personnalité juridique, vouée notamment à la protection du public auquel sont affiliés les membres de la profession et bénéficiant de prérogatives étatiques telles que le pouvoir réglementaire et le pouvoir disciplinaire. Un ordre professionnel régi par le *Code des professions* du Québec est un RPR.
- **Renouvellement** : Intervention automatique qui survient avant la date d'expiration d'un certificat valide dans le but d'en générer un nouveau pour le détenteur.
- **Révocation** : Retrait d'un certificat effectué de plein droit par le PSC/R ou à la demande d'une personne autorisée.
- **Secret partagé ou questions de sécurité** : Mot ou groupe de mots partagés sécurisés entre le PSC/R et le détenteur afin de permettre l'identification du détenteur à distance.
- **Tiers utilisateur** : Personnes agissant en se fiant à un certificat émis par l'ICP du CCQ. Il peut être ou non lui-même un détenteur de certificats de l'ICP du CCQ.

1.4 Interprétation

La CP constitue un « énoncé de politique » au sens de l'article 52 de la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ. c. C1-1).

1.5 Conformité aux normes applicables

La présente CP satisfait les exigences de l'industrie en la matière, comme celles d'eIDAS et d'ISO 27001 par exemple.

Elle définit les engagements de Notarius dans le cadre de la fourniture de services de confiance en conformité avec les normes ETSI EN 319 411-1 & ETSI EN 319 411-2.

La structure de la CP se calque sur celle du RFC 3647 (*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*¹) aux fins de meilleure compréhension.

1.6 Les composantes de l'ICP du CCQ

1.6.1 L'autorité de certification (AC)

Solutions Notarius Inc., par l'intermédiaire de son CA, agit à titre d'autorité de certification (AC). Elle s'engage notamment à :

- Adopter les modifications proposées à la CP ;
- Identifier le PSC/R ;
- Approuver les ententes prises par le PSC/R concernant les services offerts ;
- Négocier les ententes de réciprocité avec d'autres AC ou PSC/R au besoin ;

1.6.2 Le prestataire de service de certification et de répertoires (PSC/R)

L'AC a choisi au titre de PSC/R, le Comité de direction de Solutions Notarius Inc.

Ce Comité de direction est composé du Président et chef de la direction de Notarius, de la vice-présidente finances et administration (également Officier ICP), du vice-président transformation numérique, du vice-président ventes et marketing et du vice-président opérations et stratégie de produits.

Le PSC/R est responsable de l'administration quotidienne des services de certification visant la délivrance et la gestion des certificats.

Il agit également à titre d'autorité d'enregistrement (AE).

Le PSC/R est responsable :

- De proposer les mises à jour à la CP pour approbation par l'AC ;
- D'élaborer et de mettre à jour la CPS, conformément aux exigences de la CP ;
- D'identifier et de nommer les acteurs clés de l'ICP du CCQ, incluant les Officiers et les AVI ;
- Des aspects administratifs et technologiques associés à la délivrance des certificats ;
- Des opérations subséquentes reliées au cycle de vie des certificats ;
- Des services de répertoire permettant de confirmer la validité d'un certificat conformément aux exigences de l'AC ;
- De s'assurer que les vérifications nécessaires ont été effectuées avant de confirmer les éléments d'information contenus aux certificats ;
- De recueillir et consigner les renseignements relatifs aux détenteurs ;
- Délivrer des certificats dans le respect de la CP ;
- Publier la liste des certificats révoqués (LCR), celle des autorités révoquées (LAR), ainsi que les certificats publics des détenteurs ;

¹ La norme X.509 spécifie les formats pour les certificats à clé publique, les listes de révocation de certificats, les attributs de certificat. (Réf. Wikipedia.org)

-
- De s'assurer que la clé privée de l'AC ne sert qu'à signer les certificats des détenteurs, les LCR et les LAR ;
 - De mettre en œuvre des moyens nécessaires et conformes aux meilleures pratiques pour assurer la sécurité des services de répertoire ;
 - D'assurer la conservation des listes de numéros des certificats annulés et des renseignements qui y sont associés ;
 - D'assurer le support auprès des détenteurs ;
 - De déléguer certaines fonctions aux autorités locales d'enregistrement (ALE) identifiées.

1.6.3 L'autorité locale d'enregistrement (ALE)

1.6.3.1 Définition

L'autorité locale d'enregistrement (ALE) est responsable des fonctions qui lui sont déléguées par le PSC/R.

L'ALE peut être un regroupement de professionnels reconnu (RPR) par exemple un Ordre ou une association de professionnels ou encore une Personne morale.

1.6.3.2 Signature d'ententes contractuelles

Toutes les ALE ont signé des ententes contractuelles avec le PSC/R ou l'un de ses représentants autorisés par délégation de pouvoirs.

1.6.3.3 Rôles et responsabilité des ALE

L'ALE délègue formellement ses pouvoirs à des agents de vérification de l'affiliation (AVA) pour entreprise ou pour professionnels qu'elle a expressément identifiés auprès du PSC/R.

L'ALE doit :

- Avoir en tout temps aux moins deux personnes (une personne dans le cas des personnes morales) pour agir au titre d'agent vérificateur de l'affiliation (AVA) et poser les actions requises pour respecter cet élément.
- Assurer la gestion des nominations des AVA ;
- S'assurer qu'au moins un (1) AVA est disponible à chaque jour ouvrable pour remplir son rôle ;
- S'assurer que les AVA respectent les obligations identifiées dans la CP.

L'ALE ou son AVA :

- Appliquent et respectent la CP et les procédures d'utilisation du Portail de gestion, lorsqu'applicable ;
- Approuvent ou rejettent l'enregistrement des demandes initiales de certificats qui lui sont soumises en certifiant l'inscription au tableau de l'Ordre professionnel (concordance des informations nominatives fournies) ou que la personne est à l'emploi de l'ALE ;
- Révoquent la signature numérique professionnelle de tout détenteur qui ne rencontre plus les exigences de son Ordre professionnel ;
- Demandent au PSC/R de procéder à la révocation des signatures numériques corporatives de ses employés portées à son compte corporatif;
- À moins d'une entente contractuelle contraire, est le support de 1^{er} niveau auprès des

détenteurs de certificats dont elle assure la gestion.

1.6.4 Le détenteur

1.6.4.1 Définition

Le détenteur de clés et de certificats de l'ICP du CCQ est une personne physique ou une entité/un groupe/une application qui utilise son certificat pour signer, chiffrer (membres de la CNQ et de l'OAGQ uniquement) et/ou pour s'authentifier selon ses besoins ou les fonctionnalités qui lui sont disponibles.

1.6.4.2 Rôles et responsabilités

Le détenteur :

- Respecte les conditions qui lui incombent telles que définies dans la présente CP;
- Remplit les obligations relatives à son adhésion;
- Fournit les informations, pièces et documents requis;
- Protège la confidentialité de ses données d'activation, de ses données d'authentification, de sa clé privée et de son support ainsi que de son mot de passe ;
- S'assure qu'il est le seul à utiliser ses certificats ou, lorsque ceux-ci sont affectés à un groupe, un dispositif ou une application, de s'assurer qu'ils ne sont utilisés que par les personnes et les systèmes autorisés ;
- Utilise ses certificats pour les seules fins autorisées ;
- Signe en ligne ses documents pour en assurer l'authenticité ;
- Utilise son équipement informatique de façon sécuritaire;
- Avise dans les meilleurs délais le service à la clientèle du PSC/R s'il soupçonne que la confidentialité de ses clés et certificats, ou de son mot de passe, est compromis ;
- Informe le plus rapidement possible le PSC/R de tout changement ou procède lui-même aux changements requis via le libre-service « mon dossier »;
- Arrête d'utiliser ses certificats lorsque ceux-ci sont révoqués ou expirés.

1.6.5 Autres participants

1.6.5.1 Les partenaires d'affaires

Le partenaire d'affaires est une Personne morale qui désire transiger de façon électronique avec des détenteurs de certificats. Il doit être autorisé et avoir conclu une entente à cet effet avec le PSC/R.

Le partenaire d'affaires est responsable :

- D'arrimer ses processus d'affaires à l'utilisation des clés et des certificats émanant de l'ICP du CCQ;
- De se conformer aux spécifications techniques et fonctionnelles exigées par le PSC/R;
- De décider qui au sein de son organisation détiendra des clés et des certificats émanant de l'ICP du CCQ;
- D'effectuer la gestion des accès et des autorisations à ses applications informatiques;
- D'effectuer les mises à jour nécessaires pour suivre l'évolution de l'ICP du CCQ;

- D'informer les détenteurs des utilisations autorisées dans ses applications;
- De s'assurer que le détenteur a les moyens nécessaires pour respecter les obligations découlant de la Politique, entre autres, en ce qui touche l'obligation de préserver la confidentialité de ses clés privées;
- D'informer le PSC/R de tout évènement pouvant entraîner une intervention sur les clés et les certificats, notamment leur révocation.

Le PSC/R peut exiger du partenaire d'affaires qu'il se soumette à un audit ou qu'il fournisse un rapport d'audit sur des aspects qu'il détermine.

1.6.5.2 *Le tiers utilisateur*

Un tiers utilisateur est une personne qui agit en se fondant sur un certificat émis par l'ICP du CCQ. Il peut être ou non lui-même un détenteur de clés et de certificats de l'ICP du CCQ.

Le tiers utilisateur souhaitant agir en se fondant sur un certificat doit s'assurer que ce certificat :

- A été délivré par l'ICP du CCQ;
- A le niveau de confiance requis ;
- N'est pas expiré ;
- N'est pas révoqué.

1.6.5.3 *Le répondant autorisé par la Chambre des notaires du Québec (CNQ)*

Le répondant est un notaire, membre en règle de l'Ordre professionnel (hors classe C), qui a été autorisé par le PSC/R et la CNQ à vérifier l'identité du demandeur et qui doit confirmer cette vérification d'identité à l'ALE selon des procédures exceptionnelles établies.

1.7 Utilisation des clés et des certificats

1.7.1 Utilisation autorisée des clés et des certificats

Les certificats délivrés en vertu de la CP peuvent être utilisés aux fins indiquées dans le certificat lui-même et plus précisément dans le champ *key usage* ou *extended key usage*.

Selon le produit choisi, le détenteur peut utiliser ses clés et ses certificats pour l'un ou plusieurs des usages suivants :

- Confirmer son identité;
- S'authentifier auprès de services ou plateformes autorisées;
- Signer numériquement des documents électroniques afin d'en assurer l'intégrité et la non-répudiation;
- Pour les notaires et les arpenteurs géomètres du Québec seulement, chiffrer des documents afin d'assurer la confidentialité de l'information.

Chaque détenteur ou tiers utilisateur doit évaluer les circonstances et les risques associés avant de décider d'utiliser ou non un certificat délivré en vertu de la présente CP.

Le tableau suivant fournit une brève description des utilisations appropriées des signatures numériques. Les descriptions sont à titre indicatif seulement, elles se retrouvent également sur notre site Web au www.notarius.com.

Produit/Type de certificat	Utilisation appropriée
CertifiO pour professionnels	Certificat de signature numérique, certifiant l'identité et le statut professionnel du signataire. Pour l'usage exclusif du professionnel nommé dans le certificat. Le numéro de membre est indiqué dans le certificat. Nécessite une entente entre Notarius et l'ordre ou association de professionnels. Vérification de l'identité en face à face avec l'AVI du PSC/R (devant le répondant autorisé pour les notaires du Québec). Certification du statut professionnel ou du lien d'emploi
CertifiO pour employés	Certificat de signature numérique, certifiant l'identité et le lien avec l'employeur. Pour l'usage exclusif de l'individu nommé dans le certificat. Vérification de l'identité en face à face avec l'AVI du PSC/R. Certifie également le nom de l'employeur.
CertifiO pour individus (Signature Numérique – SIRF)	Certificat de signature numérique pour l'usage exclusif de l'individu nommé dans le certificat. Les SN individuelles SIRF servent plus particulièrement pour l'authentification auprès des Systèmes du Registre Foncier du Québec en ligne. Vérification de l'identité en face à face avec l'AVI du PSC/R.

1.7.2 Limite d'utilisation

L'AC et le PSC/R peuvent restreindre l'utilisation des clés et des certificats dans la mesure où les détenteurs visés en sont informés de façon explicite.

Le contrat d'adhésion, les conditions générales ou particulières d'utilisation ou les spécifications d'un produit peuvent limiter les utilisations que peut faire le détenteur de ses certificats.

Comme l'utilisation des certificats ne dépend que du comportement du détenteur, celle-ci ne garantit pas la réputation du détenteur, ni qu'il est digne de confiance ou que l'utilisation du certificat sera faite en conformité avec les lois et règlements applicables. Toutefois, les détenteurs doivent respecter strictement les usages autorisés des clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

Enfin les détenteurs s'engagent à ne plus utiliser leur certificat dès la révocation ou l'expiration de celui-ci.

1.7.3 Détenteur autorisé

Le détenteur autorisé est :

- Un membre d'un RPR ayant conclu une entente avec le PSC/R;
- Un individu agissant pour une Personne morale (employé, mandataire, etc.) qui souhaite utiliser des clés et des certificats à des fins professionnelles et au nom de cette Personne morale ;

- Toute personne physique qui désire un certificat pour ses propres besoins et qui répond aux exigences du PSC/R;
- Une personne physique qui désire transiger avec le Registre foncier du Québec en ligne.

1.8 Gestion de la CP

1.8.1 Responsable de la CP

La CP est sous la responsabilité de Solutions Notarius inc.

1.8.2 Coordonnées du responsable

Pour toute question ou remarque concernant la présente CP, les certificats émis par l'AC ainsi que tout litige, s'adresser à :

Solutions Notarius Inc.
À l'attention de la Direction générale
465 McGill, bureau 300
Montréal (Québec) H2Y 2H1
Téléphone : 514 281-1577
Courriel : Officiers@notarius.com

1.8.3 Conformité de la CP et de la CPS

Solutions Notarius Inc. via son Conseil d'administration approuve la CP.

Solutions Notarius Inc. via son Comité de direction détermine la conformité de la CPS à la CP.

La CPS sera déclarée conforme à la CP à l'issue d'un processus d'approbation des membres du Comité de direction de Notarius, pour donner suite à la révision de la CPS par l'Officier ICP et l'arrimage aux changements de la CP approuvée par l'AC.

Toute mise à jour de la CPS suivra le processus d'approbation mis en place et sera publiée pour diffusion interne seulement (classée C – Confidentiel).

Toute demande d'accès à la CPS devra être motivée auprès du PSC/R à : Officiers@notarius.com. Une réponse, favorable ou défavorable, sera renvoyée au demandeur après évaluation, le tout dans un délai raisonnable.

2 Publication et diffusion de l'information

2.1 Entités chargées de la mise à disposition des informations

Le PSC/R est en charge de la mise à disposition de la CP et des conditions générales d'utilisation. Elle met également à disposition des utilisateurs et des applications utilisatrices des certificats qu'elle émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC.

Les méthodes de mise à disposition et les adresses correspondantes sont précisées ci-après.

2.2 Informations publiées

Les informations diffusées publiquement par le PSC/R pour l'AC sont :

- La CP (<https://notarius.com/politique-de-certification/>);
- Les conditions générales d'utilisation (<https://notarius.com/informations-juridiques/>);
- Les formulaires de demande de certificat (<https://notarius.com/produits/certifio/>);
- Le certificat de l'AC racine Centre de certification du Québec;
- Les LCR valides et à jour :
 - http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl
 - http://webcrl2.notarius.net/crl/ccq_combined_crlfile1.crl
- Les LAR.
 - <LDAP://cn=CRL1,ou=AC1,o=CENTRE DE CERTIFICATION DU QUEBEC,c=CA>

Le PSC/R ne diffuse pas la CPS. Il peut cependant exceptionnellement l'autoriser sur demande expresse seulement et après évaluation de la demande (voir 1.8.3).

2.3 Délai et fréquence des publications

Les informations liées à l'ICP du CCQ sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

Les délais et fréquences de publication des informations sur l'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites ci-après :

- Le certificat de l'AC racine est publié dès que possible après son émission et doit être diffusé préalablement à toute diffusion des LCR correspondantes.
- La LCR est mise à jour et diffusée au moins toutes les deux (2) heures.
- La durée de validité de la LCR est d'un maximum de quarante-huit (48) heures.
- La CP est publiée sur le site Web de Notarius dans les meilleurs délais suivant son adoption par l'AC
- Les mises à jour apportées à la CP sont clairement identifiées à la section « Nouvelles » du site Web de Notarius.
- Si applicable, les changements apportés à la CP affectant directement les professionnels leur seront notifiés par courriel dans le respect des ententes contractuelles en place.

- La publication du statut d'un certificat par le PSC/R constitue un avis aux tiers utilisateurs. Dans cette optique, un certificat doit être considéré comme révoqué par les tiers utilisateurs dès la publication de cette information.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des détenteurs de certificats est libre d'accès en lecture.

La CP et la LCR sont accessibles en lecture à toute personne souhaitant en prendre connaissance sur le site Web de Notarius.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'ICP du CCQ, au travers un contrôle fort (basé sur une authentification à au moins deux facteurs).

3 Identification et authentification

3.1 Identification

3.1.1 Type de nom

Pour identifier un détenteur, les certificats délivrés suivent des règles d'identification et de nom. Les certificats émis par l'AC sont donc conformes aux spécifications de la norme X.509 version 3. Conséquemment, dans chaque certificat, l'AC émettrice (Issuer) et le porteur (Subject) sont identifiés par un nom distinctif, en anglais « Distinguished Name » (DN) ou (UID) « Unique ID » de type X.501.

3.1.2 Noms explicites

Les noms choisis pour désigner les détenteurs de certificats sont explicites. L'UID/DN se présente sous une des formes ci-dessous représentées en fonction du produit auquel le détenteur a adhéré :

Produit	sn	cn	ou	o	c
CertifiO pour professionnels	<i>No. de membre</i>	<i>Prénom du contact Nom du contact</i>	Nom dans le DN du compte ou Nom du compte	CENTRE DE CERTIFICATION DU QUÉBEC	CA
CertifiO pour employés	<i>Courriel professionnel Le @ remplacé par des parenthèses avant et après le domaine</i>	<i>Prénom du contact Nom du contact</i>	ou Nom de l'ALE ou CORPORATION	CENTRE DE CERTIFICATION DU QUÉBEC	CA
Signature Numérique SIRF	<i>Courriel professionnel Le @ remplacé par des parenthèses avant et après le domaine</i>	<i>Prénom du contact Nom du contact</i>	CLIENTS	CENTRE DE CERTIFICATION DU QUÉBEC	CA

3.1.3 Anonymisation ou utilisation de pseudonyme

La présente CP n'autorise pas l'utilisation de pseudonymes dans ses certificats.

3.1.4 Règles d'interprétation des différentes formes de noms

Les noms choisis pour désigner les détenteurs de certificats sont explicites. Les noms distinctifs (DN) contenus dans le champ « Subject – DN » des certificats sont interprétés selon la norme X.501 et le RFC 3280.

Les noms utilisés dans le champ CN (Common Name) des certificats correspondent aux prénom et nom du détenteur du certificat.

3.1.5 Unicité des noms

L'unicité du DN est garantie par la combinaison d'informations permettant de construire ce dernier, voir tableau ci-avant présenté.

Un DN attribué à un détenteur ne peut être attribué à un autre, et ce, durant toute la durée de vie de l'AC.

3.1.6 Identification, authentification et rôle des marques déposées

Pour les marques, dénominations sociales ou autres signes distinctifs, Notarius n'effectue aucune recherche d'antériorité ou autre vérification; il appartient au demandeur de vérifier que la dénomination demandée ne porte pas atteinte aux droits de propriété de tiers.

3.2 Validation de l'identité

L'identité d'un demandeur est vérifiée par une personne autorisée.

Les règles et les moyens acceptés pour établir l'identification du demandeur et, le cas échéant, son affiliation à un RPR ou une Personne morale sont fixés dans la CPS.

<i>Produit</i>	CertifiO pour Professionnels	CertifiO pour Employés	CertifiO pour individus (SN SIRF)
<i>Activité</i>			
<i>Type de VI</i>	DI ou RC	DI ou RC	DI ou RC
<i>Type de VA</i>	Ordre	Employeur	Aucun
<i>Certifie quoi?</i>	PN et DDN (3) Statut pro (3) Courriel (2)	PN et DDN (3) Lien emploi (3) Courriel corpo (2)	PN et DDN (3) Courriel (2)

Rôle	AVA	Officier ICP du CCQ
<i>Activité</i>		
<i>Type de VI</i>	DI ou RC	RC
<i>Type de VA</i>	Ordre/Organisation	2 Officiers
<i>Certifie quoi?</i>	PN et DDN (3) Courriel (2)	PN et DDN (3) Courriel (2)

Légende :

1. Type de VI
 - DI = À distance avec croisement de données
 - RC = Répondant de confiance en personne (ex. un employé de Notarius ou un notaire détenant une signature numérique de Notarius)
2. Niveau de fiabilité
 - 1 = affirmé par le client (self)
 - 2 = vérifié sommairement (ex. : courriel validé)
 - 3 = validé par un tiers
3. Renseignements certifiés
 - PN = Prénom et nom
 - DDN = Date de naissance

3.2.1 La vérification initiale de l'identité

La vérification initiale de l'identité est requise pour :

- Établir l'identité d'une personne physique ;
- Valider l'identité d'une Personne morale et son lien avec la personne physique.

La vérification initiale de l'identité d'une personne physique nécessite la présentation de deux pièces justificatives émanant d'une autorité gouvernementale reconnue, dont l'une, avec les prénoms(s), noms(s), date de naissance, photo et la signature du demandeur.

Les informations relatives à l'identité du demandeur et portées dans le certificat doivent correspondre exactement aux informations portées sur les éléments présentés dans le cadre de la vérification de l'identité.

La demande initiale de clé et de certificat nécessite toujours une vérification de l'identité du demandeur soit par vidéoconférence avec l'AVI du PSC/R soit en personne avec un répondant autorisé par le PSC/R et la CNQ, pour les membres de la CNQ uniquement.

Lorsqu'applicable, la vérification de l'identité des professionnels pour l'émission d'un second certificat (CertifiO pour professionnels), peut également être réalisé au moyen de leur premier certificat de signature électronique, délivré conformément au processus de vérification initiale de l'identité ci-avant expliqué. Les étapes de ce processus sont détaillées dans la CPS. Ce cas ne s'applique pas pour les membres de la CNQ.

Une fois l'identité vérifiée, l'affiliation à un RPR peut être exigée, auquel cas, ce fait devra être confirmé par le RPR concerné.

3.2.1.1 Vérification d'identité (VI) par un répondant autorisé

Pour être un répondant autorisé, la personne doit être soit:

- L'AVI du PSC/R;
- Un notaire, membre en règle de son Ordre professionnel (hors classe C) qui a été formellement désigné et autorisé par le PSC/R et la CNQ.

La vérification d'identité nécessite la complétion du formulaire spécifié accompagné de la présentation de pièces justificatives officielles émanant d'une autorité gouvernementale reconnue (voir section suivante).

La Vérification d'identité se réalise habituellement via vidéoconférence par l'AVI autorisé du PSC/R ou en personne par le répondant notaire, selon un processus détaillé dans la CPS.

Note : Les enregistrements du processus de VI réalisé par l'AVI du PSC/R incluant les copies des pièces d'identité sont chiffrés et sauvegardés dans un répertoire à accès restreint. Seuls les Officiers ICP nommés par le PSC/R ont accès à ces fichiers chiffrés. Les Officiers du PSC/R sont la V.p Finances et administration ainsi que la Chef, conformité et gestion des risques.

3.2.1.2 Liste des pièces justificatives autorisées

Les documents doivent émaner d'une autorité gouvernementale reconnue, dont l'un, avec les prénoms(s), noms(s), date de naissance, photo et la signature du demandeur afin de pouvoir être vérifiés.

La liste détaillée des pièces est exprimée sur le site Web de Notarius.

3.2.1.3 Vérification de l'affiliation par une entité autorisée

La vérification de l'affiliation doit être réalisée par un RPR ou une Personne morale détenant une entente écrite avec le PSC/R.

- Le fait pour un RPR de confirmer l'affiliation du demandeur signifie que celui-ci est un membre en règle de son Ordre professionnel ou un employé de ce RPR.
- Le fait pour une Personne morale de confirmer le lien d'emploi du demandeur signifie qu'il est autorisé à détenir des clés et des certificats portant le nom ou l'acronyme de ladite Personne morale.
- Le fait pour une Personne morale d'assumer les frais d'abonnement du détenteur équivaut également à une présomption de confirmation d'affiliation ou de lien d'emploi.

3.2.1.4 Critères d'interopérabilité

L'AC n'a aucun accord de reconnaissance avec une AC extérieure au domaine de sécurité auquel elle appartient.

3.2.2 La vérification de l'identité lors de la remise des données d'activation

Les données d'activation permettant de générer le certificat du détenteur lui sont remises par un moyen qui permet de s'assurer de son identité.

3.2.3 La vérification de l'identité lors du renouvellement d'un certificat

Le détenteur est avisé par courriel de l'expiration éminente de ses clés et ses certificats. Il doit alors s'authentifier au moyen de ceux-ci dans une application reconnue par le PSC/R pour permettre leur renouvellement.

3.2.4 La vérification de l'identité lors d'une réémission

Lorsqu'une personne demande la réémission de ses clés et ses certificats à l'intérieur d'un délai de douze (12) douze mois suivant leur révocation, leur expiration ou leur annulation, elle devra s'authentifier avec succès (à l'aide de ses questions de sécurité) au portail du PSC/R.

À défaut, le demandeur devra faire vérifier son identité selon la procédure prévue à la section 3.2.1

3.2.5 La vérification d'identité lors d'une modification

Lorsque le détenteur souhaite modifier certaines informations contenues à son certificat, il doit s'authentifier avec succès (à l'aide de ses questions de sécurité) au portail du PSC/R afin de procéder lui-même aux changements souhaités (les champs modifiables sont : le titre, le courriel professionnel, le courriel secondaire, les coordonnées téléphoniques, le pays et la province).

Tout autre changement n'étant pas autorisé via le portail du PSC/R, le détenteur devra alors communiquer avec le PSC/R (plus précisément son service à la clientèle) pour qu'une demande de modification soit ouverte en son nom.

La mise à jour de renseignements comme le prénom ou le nom nécessitera la vérification auprès du RPR du demandeur et la confirmation par écrit de ce dernier. L'Officier du PSC/R procédera, après la réception de la confirmation écrite du RPR, aux modifications demandées.

4 Gestion des clés et des certificats

4.1 Demande d'émission de clés et de certificats

4.1.1 Personnes autorisées

Une personne physique peut demander des clés et des certificats pour elle-même ou pour un groupe d'individus.

Une Personne morale peut demander des clés et des certificats pour ses employés.

4.1.2 Procédure d'adhésion

La personne autorisée qui souhaite obtenir des clés et des certificats doit:

- Faire une demande auprès du PSC/R et accepter les conditions d'utilisation;
- Acquitter les frais afférents;
- Faire vérifier son identité selon ce qui est prévu à la section 3.2;
- Se conformer à toutes autres obligations expressément portées à sa connaissance par le PSC/R

Le détail du processus est expliqué dans la CPS.

4.1.3 Approbation ou refus de la demande

À la réception d'une demande, des validations sont faites (vérification et cohérence des attestations ou documents fournis) par le PSC/R ou une ALE, qui doit l'accepter ou la refuser.

Dans tous les cas, le demandeur est avisé de la décision au moyen des informations qu'il a fournies au cours du processus d'adhésion.

4.1.3.1 *Acceptation ou refus d'une demande de signature numérique corporative*

Les demandes d'adhésion d'une signature corporative sont confirmées ou refusées par l'AVA de l'ALE, sur réception d'un courriel transmis automatiquement par le PSC/R.

La confirmation d'emploi ou le refus de la demande notifie automatiquement l'Officier du PSC/R.

Les demandes d'adhésion sont finalement traitées par l'Officier du PSC/R sur réception de la confirmation de lien d'emploi via la plateforme de gestion des signatures numériques de Notarius à accès restreint.

4.1.3.2 *Acceptation ou refus d'une demande de signature autre que corporative*

Les demandes d'adhésion sont traitées par l'AVA du RPR via la plateforme de gestion des signatures numériques de Notarius à accès restreint.

4.1.3.3 *Types de décisions pouvant être prises dans la console de gestion du PSC/R*

Trois (3) types de décisions peuvent être prises :

1. **Approuver** : approbation de la demande sélectionnée, telle quelle.
2. **Approuver avec modifications** : approbation de la demande après y avoir apporté des modifications au prénom, au nom et, lorsqu'applicable, au numéro de membre ou titre professionnel.
3. **Refuser** : refus de la demande sélectionnée en indiquant une raison (champ obligatoire).
 - Un courriel contenant la raison du refus est envoyé immédiatement au demandeur

- Un remboursement est crédité au demandeur lorsque celui-ci a payé par carte de crédit.

4.1.4 Durée de validité d'une demande

Une demande d'adhésion demeure valide et en attente d'acceptation ou de refus jusqu'à un maximum de soixante (60) jours.

Passé ce délai, la demande devient caduque et devra être refaite au complet.

4.1.5 Approbation d'un certificat

Le détenteur est notifié par courriel de l'approbation de sa demande.

Il est invité à activer sa signature numérique suite à la génération de son certificat.

Il est alors présumé avoir accepté les clés et les certificats dès leur activation.

4.2 Demande de renouvellement d'un certificat

L'opération de renouvellement du certificat est indépendante du certificat expiré.

Le service de renouvellement est complété par une notification automatique des clients lors de l'utilisation de la clé privée dans un dispositif.

Le renouvellement consiste en l'émission de nouvelles clés et de nouveaux certificats pour un même détenteur en utilisant sa clé privée existante.

Lors du processus de renouvellement, aucune nouvelle vérification d'identité ne sera requise.

L'AC émettrice peut renouveler des clés et des certificats tant que :

- Les certificats d'origine ne sont pas révoqués;
- La clé privée existante est valide et fonctionnelle;
- Les informations contenues aux certificats demeurent les mêmes;

Aucune validation ou vérification supplémentaire n'est nécessaire.

4.2.1 Personnes autorisées

Le processus de renouvellement d'un certificat peut être initié au choix par :

- Une application;
- Un dispositif;
- Par le détenteur lui-même lors de l'utilisation de sa clé privée

4.2.2 Procédure de demande de renouvellement d'un certificat

En fonction des *certificates policies*, la période de validité des certificats délivrés par l'AC peut être de 24, de 36 mois ou plus à partir de leur date d'émission.

Le processus de renouvellement débute à un certain pourcentage de durée de vie du certificat (informations également disponibles dans les *certificates policies*).

Le processus est initié automatiquement par le détenteur lors de l'utilisation de sa clé privée dans un dispositif.

4.2.3 Traitement d'une demande de renouvellement d'un certificat

Le processus de renouvellement du certificat est initié automatiquement par le détenteur lui-même 30 jours avant la date d'expiration de sa clé privée dans les cas où l'utilisateur utilise sa signature numérique en ligne.

Lors du renouvellement, il est nécessaire de :

- Authentifier le détenteur au moyen de sa clé privée;
- Générer des clés et des certificats signés par l'AC et les transmettre au détenteur.

4.2.4 Avis de renouvellement

Quatre (4) avis de renouvellement sont envoyés par courriel au détenteur du certificat à des échéances planifiées. Les traces de ces avis sont conservées dans son dossier client.

Le détenteur est notifié dès la génération de son certificat par le dispositif.

4.3 Récupération d'un certificat

La récupération consiste en l'émission de nouvelles clés et de nouveaux certificats alors que la clé privée existante est valide, mais non fonctionnelle, notamment en raison de la perte du mot de passe liée à la clé privée ou de la destruction des clés.

L'AC émettrice peut récupérer des clés et des certificats tant que :

- La clé privée existante est valide;
- Le détenteur peut s'authentifier auprès du PSC/R;
- Les informations contenues aux certificats demeurent les mêmes

4.3.1 Personnes autorisées

L'AC émettrice peut accepter une demande de récupération amorcée par le détenteur lui-même ou une personne ayant un rôle de confiance (voir section 5.2.1).

4.3.2 Procédure de récupération

Différents types de procédures de récupération peuvent se présenter.

- En ligne
- En personne

4.3.3 Traitement d'une demande de récupération

Le processus est initié par le détenteur lui-même, en s'authentifiant auprès d'un dispositif lui permettant d'effectuer l'opération.

Autrement, le processus doit être initié par une personne ayant un rôle de confiance; le détenteur reçoit alors une notification et les instructions nécessaires pour procéder à la récupération au moyen d'un dispositif approprié.

4.3.3.1 Récupération en ligne

La récupération en ligne est celle initiée par le détenteur du certificat via le LS (avec une VI en ligne).

4.3.3.2 Récupération en personne

La récupération en personne consiste à refaire le processus d'adhésion à la signature numérique (voir 4.1).

4.4 Demande de modification d'un certificat

La modification consiste à apporter des changements dans les informations contenues aux certificats, pourvu que la clé privée existante soit encore valide et fonctionnelle.

4.4.1 Personnes autorisées

Le processus est initié par le détenteur lui-même ou par une personne ayant un rôle de confiance (voir section 5.2.1). Le détenteur reçoit alors une notification et les instructions nécessaires pour

confirmer les changements apportés.

4.4.2 Circonstances pouvant entraîner une modification

Une modification peut avoir lieu pour corriger une erreur d'orthographe ou changer un renseignement non critique contenu dans le certificat.

4.4.3 Traitement d'une demande de modification

Le détenteur peut procéder lui-même à la modification de certains renseignements non critiques contenus dans ses certificats. Il doit alors s'authentifier à l'aide de ses questions secrètes au LS et effectuer les changements lui-même.

Autrement, une demande de modification écrite du détenteur doit être acheminée au PSC/R afin qu'il puisse procéder en son nom ou transférer la demande à l'AVA de l'ALE pour que celui-ci approuve la demande de modification.

4.4.4 Avis de modification

Le détenteur doit utiliser sa clé privée dans un dispositif pour être notifié et constater les modifications apportées.

4.5 Révocation d'un certificat

4.5.1 Causes possibles d'une révocation

4.5.1.1 Certificats des détenteurs

La révocation consiste à rendre les clés et les certificats d'un détenteur inutilisables et d'ajouter le numéro de série des certificats à la LCR.

L'inscription à la LCR signifie au tiers que le cycle de vie des certificats a pris fin.

Les circonstances suivantes peuvent être à l'origine de la révocation du Certificat de signature du détenteur :

- Le Certificat est devenu obsolète par suite d'un changement des données du client figurant dans le certificat;
- Les informations du client figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat
- Le détenteur n'a pas respecté les modalités applicables d'utilisation du certificat;
- Le client, l'ALE, le RPR ou l'AC n'ont pas respecté leurs obligations découlant de la CP;
- Une erreur importante (intentionnelle ou non) a été détectée dans le dossier client du détenteur;
- La clé privée du détenteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées);
- Le détenteur ou un responsable autorisé demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du détenteur);
- Le certificat de signature de l'AC est révoqué (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante);
- Le décès du détenteur ou la cessation d'activité de son employeur;
- Le détenteur n'est plus un membre en règle d'un Ordre professionnel (condition d'émission du certificat);
- Fin de relation contractuelle entre l'AC et le Client du Service – et donc avec ses Utilisateurs – avant la fin de validité des certificats.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC ou le PSC/R en a connaissance

(elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau Certificat notamment), le Certificat concerné est révoqué.

Le PSC/R peut également, à sa discrétion, révoquer un certificat lorsque son détenteur ne respecte pas les obligations énoncées dans la CP. Cela ne s'applique toutefois pas aux certificats de signature numérique émis aux notaires où l'approbation du Secrétaire de l'Ordre est requise (cas des révocations pour non-paiement des frais).

4.5.1.2 Certificats d'une composante de l'ICP DU CCQ

Plusieurs circonstances peuvent être à l'origine de la révocation d'un certificat d'une composante de l'ICP du CCQ (incluant un certificat de l'AC pour la génération de certificats et de LCR) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'ICP du CCQ à la suite de la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la CPS (par exemple, à la suite d'un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.5.2 Origine d'une demande de révocation

4.5.2.1 Certificats des détenteurs

Les personnes ou entités qui peuvent demander la révocation du certificat d'un détenteur sont les suivantes :

- Le détenteur du certificat lui-même
- L'AC émettrice du certificat ou un membre de son personnel
- L'ALE ou le RPR

Dès qu'une personne ou une entité a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, elle doit formuler sa demande de révocation sans délai.

4.5.2.2 Certificats d'une composante de l'AC

La révocation d'un certificat d'AC ne peut être décidée que par le CA de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.5.3 Personnes autorisées à révoquer les certificats des détenteurs

Les personnes autorisées à révoquer des certificats sont :

- Le détenteur lui-même
- Le représentant autorisé du RPR pour les signatures professionnelles
- L'Officier du PSC/R

4.5.4 Traitement d'une demande de révocation

4.5.4.1 *Révocation des certificats des détenteurs*

La demande de révocation est faite auprès de l'AC émettrice et est signée avec le certificat ayant servi à effectuer l'opération.

Les demandes de révocation sont traitées en urgence, au maximum dans le prochain jour ouvrable. Il s'écoule un maximum de 5 minutes entre le traitement de la révocation et la publication de la nouvelle LCR prenant en compte ce traitement.

Les détails des étapes de traitement sont exprimés dans la CPS.

4.5.4.2 *Révocation des certificats d'une composante de l'ICP du CCQ*

La CPS précise les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'ICP du CCQ.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des clients concernés que leur certificat n'est plus valide.

4.5.5 Avis de révocation

Le détenteur reçoit un avis de révocation aussitôt l'opération effectuée dans les cas de révocation d'un certificat déjà activé.

Advenant le cas où le certificat révoqué n'ait jamais été activé, aucune notification ne sera transmise au détenteur. Une trace sera toutefois laissée dans son dossier client.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informera dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides.

4.6 Suspension d'un certificat

La suspension de certificat n'est autorisée ni par la CP ni par la CPS.

5 Mesures de sécurité physique et opérationnelle

Le PSC/R s'engage à mettre en œuvre et maintenir le niveau de sécurité physique exigé pour les locaux d'exploitation des composantes de l'ICP du CCQ.

5.1 Mesures de sécurité physique

La CP indique les mesures qui doivent être mises en place par le PSC/R pour assurer la sécurité physique de l'ICP du CCQ. Cela couvre notamment les contrôles d'accès physique, la protection en cas de catastrophe naturelle, les pannes de services, protection contre le feu, le vol et les inondations. Les contrôles doivent être mis en œuvre pour éviter la perte, les dommages, les interruptions des activités commerciales ou la compromission des actifs informationnels, ainsi que les activités à faire pour la reprise après sinistre. Les exigences définies ci-après sont les exigences minimales à respecter. Elles sont plus amplement détaillées dans la CPS.

5.1.1 Situation géographique des sites

Le PSC/R veille à ce que les informations critiques et sensibles soient situées dans des zones sécurisées. Les protections envisagées sont proportionnelles aux risques identifiés dans l'analyse de risque.

Les sites où sont entreposés les systèmes informatiques de l'ICP du CCQ sont dans des édifices géographiquement situés à plusieurs kilomètres l'un de l'autre.

Ces sites respectent les règlements et normes en vigueur ainsi que les mesures de sécurité physique pour la protection périphérique, périmétrique et intérieure et notamment les mesures relatives à :

- L'alimentation électrique et climatisation ;
- La vulnérabilité aux dégâts des eaux ;
- La prévention et protection incendie.

Les mesures permettent également de respecter les engagements pris dans la CP ou dans les engagements contractuels avec les Clients, en matière de disponibilité des services.

5.1.2 Accès physique

Les installations de l'ICP du CCQ sont contrôlées et vérifiées de sorte que seules les personnes autorisées puissent avoir accès aux systèmes et aux données.

Toute personne non autorisée à accéder à une zone sécurisée doit toujours être accompagnée par un employé autorisé.

En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

De plus, le contrôle en entrée et en sortie est permanent en heures non ouvrées.

Chaque entrée et sortie dans la zone sécurisée fait l'objet d'une surveillance indépendante.

Tout personnel non autorisé doit obligatoirement être accompagné d'une personne autorisée.

Chaque entrée et sortie fait l'objet d'une traçabilité.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'ICP du CCQ définissent un périmètre de sécurité physique où sont installées ces machines. L'ouverture de la porte est commandée par un système de contrôle d'accès. Les AC racines sont opérées dans un espace physiquement isolé des autres opérations. L'accès à cet espace doit permettre son accès qu'aux personnes autorisées à accéder aux clés de l'AC racine.

Voir la CPS pour le détail.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'AC telles que fixées par leurs fournisseurs. Les sites sont équipés d'un système électrique principal et d'un système de secours afin d'assurer un accès continu et ininterrompu à l'électricité. De plus, ils sont équipés d'un système principal et secondaire de ventilation ou d'air conditionné afin de contrôler la température et l'humidité relative.

5.1.4 Vulnérabilité aux dégâts d'eau

Les moyens de protection mis en place par l'AC permettent de protéger son infrastructure contre les dégâts des eaux.

5.1.5 Prévention et protection contre les incendies

L'AC met en place des moyens de protection et de lutte contre les incendies.

5.1.6 Conservation et protection des supports

Les supports utilisés au sein de l'AC sont traités et conservés conformément aux besoins de sécurité en termes de confidentialité, d'intégrité et de disponibilité.

Les supports font l'objet de mesures contre les dommages, le vol, les accès non autorisés et l'obsolescence. Ces mesures s'appliquent durant toute la période de rétention de leur contenu. Les moyens de conservation permettent donc de respecter les engagements pris par l'AC en matière de restitution et de pérennité de l'archivage.

5.1.7 Mise hors service des supports

En fin de vie, les supports seront, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes. Les procédures et moyens de destruction et de réinitialisation sont conformes à la politique de sécurité de Notarius. Les sauvegardes sont testées régulièrement.

5.1.8 Prise de copie

Des sauvegardes suffisantes du système et des applications logicielles essentielles sont conservées hors sites pour permettre le rétablissement du service à la suite d'une défaillance du système ou un sinistre.

Ces sauvegardes testées régulièrement sont organisées de façon à assurer une reprise des services après incident la plus rapide possible.

5.1.9 Relève

En complément de sauvegardes sur sites, le PSC/R met en œuvre des sauvegardes hors sites des applications de l'ICP du CCQ et de leurs informations. Ce système de relève garantit le maintien du service et des informations advenant une défaillance du système principal et des logiciels essentiels à la livraison des services de l'ICP du CCQ après un sinistre ou une défaillance du support de stockage.

5.2 Mesures de sécurité opérationnelle

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la bi clé de l'AC.

Les procédures et politiques de sécurité sont communiquées aux employés.

Des procédures sont établies et appliquées pour toutes les opérations du personnel ayant un rôle de confiance pouvant impacter la fourniture du service.

La CPS indique les mesures et les contrôles opérationnels et administratifs devant être mis en place par le PSC/R pour assurer la sécurité des opérations de l'ICP du CCQ.

5.2.1 Rôles de confiance

L'administration de l'ICP du CCQ comporte des rôles de confiance assurant une répartition des tâches de façon qu'il n'y ait pas de conflit d'intérêts possible et qu'une personne ne puisse agir seule et contourner la sécurité du système de l'ICP du CCQ.

L'AC distingue notamment les rôles suivants :

- **Officier de la sécurité** : Responsable de l'administration globale et de la mise en œuvre des pratiques de sécurité.
- **Gestionnaire des opérations** : Responsable de certaines opérations sur les certificats. Par exemple, ce rôle permet d'accéder au Security Manager et de procéder aux opérations d'inscription, de récupération et de révocation des signatures numériques.
- **Administrateur ICP du CCQ** : Responsable de l'administration et de l'exploitation des systèmes de l'ICP du CCQ. Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'entité. Il assure l'administration technique des systèmes et des réseaux de l'entité.
- **Auditeur Audit Log** : Individu autorisé à procéder aux audits mensuels des logs de l'ICP du CCQ.
- **Agent vérificateur de l'identité (AVI)** : Responsable de vérifier et confirmer auprès du PSC/R l'identité d'un demandeur.
- **Agent vérificateur de l'affiliation (AVA)** : Responsable de vérifier et de confirmer auprès du PSC/R l'affiliation associative d'un demandeur ou son affiliation d'emploi avec une Personne morale. L'AVA confirme cette vérification en approuvant ou refusant une demande d'émission d'un certificat.
- **Détenteur de carte HSM** : Responsable de détenir une carte HSM nécessaire pour le fonctionnement du module matériel d'entreposage des clés de l'AC.
- **Répondant autorisé de la CNQ** : Autorise les notaires à utiliser une signature officielle numérique et peut révoquer cette autorisation en fonction des lois, règlements et contrats en vigueur.

Un même rôle fonctionnel peut être tenu par plusieurs personnes.

Des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture du service de certification.

Ces rôles sont inclus dans la description des postes des employés du PSC/R.

Des mécanismes de contrôles d'accès appropriés sont en place.

5.2.2 Nombre de personnes requises par tâche

Le nombre de personnes requises par tâches selon le type d'opération effectuée, le nombre et la

qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, est précisé dans la CPS ou dans des procédures internes du PSC/R.

5.2.3 Identification et authentification pour chaque rôle

L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants que ce soit à l'entrée en fonction du poste que lors de l'attribution de nouvelles responsabilités en lien avec ces rôles de confiance, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant les systèmes concernés par le rôle;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes;
- Qu'un compte soit ouvert à son nom dans ces systèmes;
- Que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'ICP du CCQ.

Ces contrôles sont décrits dans la CPS de l'AC et sont conformes à la politique de sécurité de Notarius.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des services offerts ou encore que le risque ait été accepté par le RSI de l'AC.

Un rôle de confiance peut également être porteur d'une part de secret. Une personne ne peut cumuler plusieurs rôles de confiance dont les secrets sont, réellement ou en apparence, inconciliables entre eux.

5.2.5 Analyse de risque

Notarius réalise une analyse de risque afin d'identifier les menaces sur l'ICP du CCQ. Cette analyse est revue au moins une fois par année ou lors de changements structurels significatifs.

5.3 Mesures de sécurité relatives au personnel

5.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein du PSC/R est soumise au respect de procédures strictes de confidentialité et de respect d'exigences de sécurité de l'information. Le responsable des ressources humaines s'assure que les attributions de ses personnels, amenés à travailler au sein de l'ICP du CCQ, correspondent à leurs compétences professionnelles. Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur ainsi que des mesures de protection des données personnelles.

5.3.2 Vérifications des antécédents

Avant de nommer une personne à un rôle de confiance, une vérification de ses antécédents judiciaires est faite.

La CPS décrit les procédures utilisées pour identifier et authentifier les personnes nommées à un rôle de confiance. Ces dernières ne doivent pas souffrir de conflit d'intérêts préjudiciables à

l'impartialité de leurs tâches.

5.3.3 Formation initiale

Les personnes qui occupent des fonctions reliées à la prestation de services de l'ICP du CCQ ont reçu la formation appropriée pour accomplir leurs tâches. Elles sont préalablement formées aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'elles mettent en œuvre et qu'elles doivent respecter. Les personnes occupant des rôles de confiance ont connaissance et comprennent les implications des opérations dont elles ont la responsabilité.

5.3.4 Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux personnes occupant des rôles de confiance dans la mesure où cette évolution impacte leur mode de travail.

Ces personnes sont également formées à la gestion des incidents et du processus de déclaration et d'escalade.

5.3.5 Fréquence et séquence de rotations entre différentes attributions

Sans objet

5.3.6 Mesures disciplinaires

Des procédures disciplinaires sont en place et des sanctions appropriées sont appliquées lorsqu'un employé ne respecte pas les procédures et politiques de sécurité applicables ou encore les dispositions de la CP ou de la CPS.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont documentées par contrat écrit.

Le personnel des prestataires externes intervenant dans les locaux de Notarius et/ou sur les sites de relève respecte également les exigences du présent chapitre 5.3.

5.3.8 Documentation fournie au personnel

La CP, la CPS, les procédures et processus qui en découlent ainsi que les autres documents (manuel d'utilisation, etc.) pertinents sont mis à la disposition du personnel occupant des fonctions reliées à la prestation de services de l'ICP du CCQ. Plus spécifiquement, les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant.

5.4 Procédure de journalisation (Registre des vérifications)

La journalisation d'événements consiste à enregistrer des événements sous forme manuelle ou sous forme électronique par saisie ou par génération automatique. Les fichiers résultants doivent rendre possibles la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'évènement enregistré

Plusieurs types d'évènements sont enregistrés.

Globalement, les événements relatifs à la sécurité et aux services d'ICP du CCQ sont collectés; tous les journaux d'audit de sécurité sont conservés et mis à disposition lors des audits de conformité; les événements liés au cycle de vie des certificats sont enregistrés de manière à assurer la traçabilité des actions effectuées par une personne ayant un rôle de confiance.

Précisément (liste non exhaustive) :

- Évènements automatiquement enregistrés:
 - Création / modification / suppression des données d'authentification correspondantes;
 - Démarrage et arrêt des systèmes informatiques et des applications;
 - Ceux liés à la journalisation;
 - Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes;
 - Arrêt inopiné ou détection d'erreurs matérielles du système;
 - Activité des routeurs et des firewalls.

- Évènements nécessitant une intervention manuelle:
 - Accès physiques;
 - Maintenance et/ou configuration des systèmes;
 - Destruction des supports.

- Évènements spécifiques aux différentes fonctions:
 - Réception, approbation ou refus d'une demande de certificat;
 - Évènements liés aux clés de signature et aux certificats d'AC;
 - Publication et mise à jour des informations liées à l'AC;
 - Génération des clés et des certificats des détenteurs;
 - Traitement des demandes de révocation;
 - Génération et publication des LCR.

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'évènement.

5.4.2 Fréquence des vérifications des registres

Les registres de vérifications sont analysés périodiquement. De plus, les journaux d'évènements font l'objet d'analyses automatiques permettant d'identifier des activités anormales et alerter les personnels de l'occurrence potentielle d'évènements critiques de sécurité.

5.4.3 Conservation des registres des vérifications

Les registres de vérifications sont conservés pendant une période de temps appropriée permettant de fournir, le cas échéant, les preuves juridiques nécessaires en fonction de la législation applicable.

5.4.4 Mesures de protection

Les registres de vérification sont protégés en tout temps de manière à empêcher leurs altérations et afin d'en assurer la confidentialité, l'intégrité et la disponibilité. Ils sont enregistrés pour faire en sorte qu'ils ne soient ni supprimés ni détruits pour la période où ils doivent être conservés.

5.4.5 Évaluation des vulnérabilités

Des mesures sont en place pour effectuer des évaluations des vulnérabilités afin de diminuer ou d'éliminer les menaces touchant les actifs de l'ICP du CCQ.

5.5 Conservation et archivage des données

5.5.1 Types de données à conserver et archiver

L'archivage permet d'assurer la pérennité des journaux de l'ICP du CCQ. Il permet également la conservation des pièces liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité. Les données à archiver sont au moins les suivantes :

- La CP;
- La CPS;
- Les certificats, LCR et réponses OCSP;
- Les registres de vérification;
- Les données du répertoire;
- Les médias d'installation des systèmes d'exploitation, des applications de l'ICP du CCQ et du répertoire ;
- La base de données de l'application du PSC/R servant à la gestion des données détenteurs;
- Les dossiers clients.

5.5.2 Périodes de conservation des archives

Les durées d'archivage sont notamment les suivantes :

- Les renseignements recueillis pour établir l'identité des détenteurs : minimum 10 ans de la vérification.
- Les certificats et la clé publique de signature ainsi que les clés et les certificats de chiffrement : minimum 10 ans après la révocation ou l'expiration des clés et des certificats d'un détenteur.
- Les copies de sauvegarde des données : de 1 mois à 10 ans, selon les données concernées.

Notarius a mis en place un calendrier de conservation détaillé ainsi que des mesures nécessaires pour que ces archives soient conservées sur les durées mentionnées.

5.5.3 Protection des archives

Les archives sont enregistrées afin qu'elles ne puissent être supprimées ou détruites pendant leur période de conservation. Les mesures de protection des archives en place assurent que seules les personnes autorisées peuvent y avoir accès et les manipuler sans en modifier l'intégrité, la confidentialité et l'authenticité des données. Ces archives sont lisibles et exploitables sur l'ensemble de leur cycle de vie.

Des procédures de conservation, de destruction et de transfert des données sont en place et détaillées dans la CPS.

5.5.4 Exigence d'horodatage des données

Les certificats sont datés au moment de leur génération et cette information est archivée avec le certificat correspondant. La section 6.8 précise les exigences en matière de datation ou d'horodatage.

5.5.5 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données. La CPS précise les moyens mis en œuvre pour collecter les archives en toute sécurité.

5.5.6 Procédure de récupération et de vérification des archives

Les archives doivent pouvoir être récupérées dans un délai maximal de 24 h. Les conditions de récupération des archives sont précisées dans la CPS.

5.6 Changement de clés d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé, et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise par suite d'une compromission ou d'un sinistre

5.7.1 Procédure de remontée et de traitement des incidents et des compromissions

Le PSC/R met en œuvre des procédures et des moyens de remontée et de traitement des incidents conformément aux exigences de la politique de sécurité de Notarius. Ces moyens permettent de minimiser les dommages en cas d'incidents.

5.7.2 Procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)

Conformément à la politique de sécurité de Notarius, un plan de continuité des affaires est mis en place permettant de répondre aux exigences de disponibilité des fonctions sensibles découlant notamment de la présente CP mais également du respect des engagements notamment pour ce qui touche les fonctions liées à la publication ou la révocation des certificats. Ce plan est testé au minimum une fois tous les 2 ans.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'une composante de l'ICP du CCQ est traité conformément au chapitre 5.7.2 « Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données) ».

En particulier, en cas de compromission d'une clé d'AC, le PSC/R de Notarius:

- Informera tous les détenteurs de certificats impactés, ainsi que les tiers utilisateurs avec lesquels l'AC a passé des accords;
- Indiquera que les certificats émis par l'AC, ainsi que les statuts de révocation publiés, ne sont plus valides;
- Révoquera immédiatement tous les certificats concernés.

5.7.4 Capacités de continuité d'activité suite à un sinistre

La capacité de continuité d'activité suite à un sinistre est traitée à même le plan de continuité des affaires (CPA) de Notarius. Ce CPA décrit les étapes à suivre pour remettre à disposition les activités de l'ICP du CCQ, totalement ou en mode dégradé, ainsi que la reprise éventuelle de l'exploitation normale des services après réfection ou le remplacement des ressources détruites ou endommagées.

5.8 Cessation des activités

5.8.1 Cessation des activités de l'AC

L'AC doit aviser le PSC/R et les ALE au moins six (6) mois à l'avance de son intention de mettre fin à ses activités en tant qu'autorité de certification.

Les modalités de transfert des opérations et des responsabilités à un tiers sont décidées entre l'AC et le PSC/R et sont ensuite communiquées aux ALE. Les engagements sont détaillés dans la CPS.

5.8.2 Cessation des activités du PSC/R

Le PSC/R doit aviser l'AC et les ALE au moins trois (3) mois à l'avance de son intention de cesser ses activités. Les modalités de transfert doivent être approuvées par l'AC et sont ensuite communiquées aux ALE.

Le PSC/R prendra les dispositions nécessaires pour transférer les dossiers et les données à un autre prestataire de services de certification et de répertoire désigné par l'AC.

5.8.3 Cessation des activités de l'ALE

Dans la mesure du possible, l'ALE doit aviser le PSC/R au moins trois (3) mois à l'avance de son intention de cesser ses activités.

5.8.4 Fin de vie de l'Infrastructure de gestion des clés

La compromission de la clé de l'AC entraînerait immédiatement sa cessation d'activité et la révocation de tous les certificats émis en cours de validité. Pour retrouver le niveau de service, la création d'une nouvelle AC et de nouveaux certificats serait obligatoire.

6 Mesures de sécurité techniques

Les exigences ci-après définies sont les exigences minimales que l'AC respecte.
Ces exigences sont complétées puis déclinées en mesures de sécurité spécifiées dans la CPS.

6.1 Génération et livraison des clés

6.1.1 Génération des clés

6.1.1.1 Clés de l'AC

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre d'une « Cérémonies des Clés »

Lorsque les paires de clés de l'AC racine sont générées, elles le sont en présence d'au moins deux personnes occupant un rôle de confiance d'Officier de la sécurité ou de Gestionnaires des opérations.

La cérémonie fait l'objet d'un PV signé attestant qu'elle s'est déroulée conformément à la procédure prévue et démontrant que l'intégrité et la confidentialité de la génération de la paire de clés ont été assurées.

6.1.1.2 Clés des détenteurs générées par l'AC

La génération des clés des détenteurs est effectuée dans un environnement sécurisé. Les clés sont générées dans un module cryptographique conforme aux exigences légales, réglementaires ou normatives applicables.

6.1.1.3 Clés des détenteurs générées par les détenteurs

Sans objet

6.1.2 Transmission de la clé privée à son propriétaire

Les clés sont générées sur le poste de travail du détenteur ou sur un dispositif cryptographique matériel avec l'application du PSC/R.

Une fois remise, la clé privée est maintenue sous le seul contrôle du détenteur.

L'AC ne conserve ni ne duplique cette clé privée.

6.1.3 Transmission de la clé publique de l'AC aux utilisateurs de certificats

La clé publique de signature de l'AC est mise à disposition des détenteurs et des tiers utilisateurs et peut être consultée publiquement. Elle est protégée en intégrité et son origine authentifiée lorsqu'elle est transmise de et vers l'AC Serveurs.

6.1.4 Taille des clés

La taille des clés des AC est de 4096 bits.

La taille des clés des détenteurs est de 2048 bits.

6.1.5 Vérification de la génération des paramètres des clés et de leur qualité

Les paramètres et les algorithmes de signature mis en œuvre dans les boîtiers crypto, les supports matériels et logiciels sont documentés par l'AC.

L'équipement de génération des clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la clé.

6.1.6 Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC et du certificat associé est exclusivement limitée à la signature de certificats d'AC et de LCR.

L'utilisation de la clé privée du détenteur et du certificat associé est strictement limitée au service de signature.

6.2 Normes de sécurité relatives aux modules cryptographiques et protection des clés privées

6.2.1 Normes de sécurité relatives aux modules cryptographiques

Les modules servant à la génération des clés ainsi qu'aux opérations cryptographiques satisfont les standards reconnus par l'industrie. En effet, les modules servant à la génération des clés ainsi qu'aux opérations cryptographiques sont conformes aux spécifications FIPS-140-2 reconnues par la *National Institute of Standards and Technology* (NIST) et adoptées par le Centre de la sécurité des télécommunications Canada (CST). La série de publication FIPS-140 définit les requis et standards pour les modules cryptographiques logiciels et matériels. Le FIPS 140-2 assure la protection des clés avec un niveau de sécurité jugé acceptable au regard des menaces pesant sur l'intégrité, la disponibilité et la confidentialité.

6.2.2 Protection des clés privées de l'AC (contrôle des clés privées de l'AC par plusieurs personnes)

Les clés privées de l'AC doivent être entreposées dans un dispositif matériel certifié FIPS 140-2 niveau 3 ou plus.

L'intervention conjointe de deux employés occupant un rôle de confiance approprié est requise pour les opérations relatives aux clés privées de l'AC.

6.2.3 Séquestre de la clé privée

Les clés privées des détenteurs ne font pas l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

Une copie de la clé privée de déchiffrement peut être conservée par l'AC émettrice en prévision d'une éventuelle récupération, pourvu que des mesures de sécurité appropriées soient en place pour en préserver l'intégrité.

6.2.5 Archivage de la clé privée

Les clés privées des détenteurs ne doivent en aucun cas être archivées ni par l'AC ni par aucune des composantes de l'ICP du CCQ.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Le transfert de la clé privée du détenteur vers le support cryptographique se fait conformément aux exigences de la section 6.1.1.2

6.2.7 Stockage de la clé privée dans le module cryptographique

Les clés privées des détenteurs sont protégées par leurs modules cryptographiques.

6.2.8 Contrôle multi-usager (m de n)

Le contrôle des clés privées de signature de l'AC est assuré par deux (2) personnes au minimum occupant un rôle de confiance en suivant la méthode d'authentification m de n.

6.2.9 Protection des clés privées du détenteur

Le détenteur est seul responsable de la protection de ses clés privées.

En ce sens, il doit prendre toutes les mesures nécessaires pour assurer la sécurité et la confidentialité de ses clés privées, notamment en choisissant un mot de passe respectant certains critères portés à sa connaissance par le PSC/R.

6.2.10 Méthode d'activation de la clé privée

6.2.10.1 Activation de la clé privée de l'AC

L'activation de la clé privée de l'AC ne peut être effectuée que par la personne autorisée, et nécessite la présence de deux personnes au moins.

6.2.10.2 Activation de la clé privée des détenteurs

L'activation de la clé privée du détenteur est contrôlée via des données d'activation. Plus de détails sont spécifiés dans la CPS.

6.2.11 Méthode de désactivation de la clé privée

6.2.11.1 Désactivation de la clé privée de l'AC

Cette question est traitée dans d'autres documents spécifiques à l'ICP du CCQ. En effet, les modalités de désactivation sont propres à la technologie du module; elles sont détaillées dans la documentation du constructeur.

6.2.11.2 Désactivation de la clé privée des détenteurs

Sans objet.

6.2.12 Méthode de destruction des clés privées

6.2.12.1 Destruction de la clé privée de l'AC

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.12.2 Destruction de la clé privée des détenteurs

La clé privée des détenteurs doit être automatiquement détruite dès lors que le certificat associé à cette clé a expiré. Cette clé est alors systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.3 Autres aspects relatifs à la gestion des clés et des certificats

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des détenteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 Durées de vie des clés et des certificats

Par principe, la durée de vie opérationnelle d'un certificat est limitée par son expiration ou sa révocation.

L'AC Serveurs ne peut pas émettre des certificats porteurs dont la durée de vie est supérieure à celle de son certificat.

Les périodes d'utilisation des clés émises sont :

Type	Durée maximale de vie – avant expiration du certificat
AC Racine	20 ans
AC Émettrice	20 ans
Clé de signature	3 ans
Clé de chiffrement	3 ans
Clé de test	1 an
Service OCSP (Online Certificate Status Protocol / Protocole de vérification en ligne)	2 ans

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation utilisées pour l'émission de l'AC racine ou d'une AC émettrice et leur entreposage dans un module matériel doivent être faites dans le cadre d'une cérémonie des clés. Les données d'activation pour les détenteurs sont accessibles uniquement après que celui-ci se soit identifié auprès du PSC/R, notamment en accédant au site Web de Notarius et en s'authentifiant à l'aide des réponses aux questions de sécurité recueillies lors de son adhésion à un produit/type de certificat. La remise des données d'activation est donc séparée dans le temps ou dans l'espace de la remise de la clé privée.

6.4.2 Protection des données d'activation

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'ICP du CCQ sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité. Les données d'activation qui sont générées par l'AC pour les partitions cryptographiques des détenteurs sont protégées en intégrité et en confidentialité jusqu'à la remise au destinataire. Ce dernier a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.5 Mesures de sécurité informatiques

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de

contrôle est cohérente avec la politique de sécurité de Notarius.

Pour atteindre ces objectifs de sécurité, l'utilisation de systèmes et de produits fiables permet de mettre en œuvre de façon sécurisée les différents processus de l'ICP du CCQ. Les systèmes et produits sont choisis ou développés en prenant en compte les exigences de sécurité.

Les mesures de sécurité informatique, définies dans la CPS, répondent notamment aux objectifs de sécurité suivants:

- Identification et authentification des utilisateurs pour l'accès au système ;
- Gestion des sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression des droits d'accès ;
- Protection du réseau contre les intrusions et pour l'assurance de la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits.

6.6 Mesures de contrôle

Des mesures de contrôles, définies dans la CPS, sont en place pour assurer le niveau de confiance de l'ICP du CCQ, notamment :

- Documenter toute modification ou évolution de l'ICP du CCQ;
- Enregistrer les mises à niveau appliquées à l'ICP du CCQ;
- L'audit des journaux d'activités;
- L'audit de l'intégrité et de la disponibilité de l'ICP du CCQ.

Afin de s'assurer du maintien du niveau de confiance, le PSC/R réalise une analyse globale des risques des composantes faisant partie ou visant à supporter les services offerts par l'ICP du CCQ. Lors de l'installation, et de manière périodique, le PSC/R vérifie également l'intégrité de ses systèmes.

6.7 Mesures de sécurité réseau

L'AC s'engage à ce que les réseaux utilisés dans le cadre de l'ICP du CCQ respectent les objectifs de sécurité informatiques définis dans la CPS. Elle applique notamment les règles suivantes :

- Élaboration et mise à jour d'un schéma d'architecture réseau;
- Interdiction d'interconnexion d'équipements personnels;
- Mise en place de réseaux cloisonnés;

6.8 Horodatage et système de datation

Les systèmes de datation sont synchronisés via une source fiable du temps universel (UTC) et d'un serveur Network Time Protocol (NTP) avec une précision au moins égale à une minute. Toutes les composantes de l'AC incluant les serveurs de l'ICP du CCQ sont donc régulièrement synchronisées avec ce serveur de temps. Les informations fournies sont utilisées pour établir une datation sûre de :

- Début de validité d'un certificat de l'AC;

- Début de la révocation d'un certificat de l'AC;
- De l'affichage des mises à jour de LCR;
- De l'inscription des évènements dans les journaux.

7 Profils des certificats, de l'OCSP, du TSA et des LCR

7.1 Profil des certificats

L'AC émet des certificats dans un format conforme aux spécifications de la norme X.509, version 3 décrite dans la RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile ».

Dans chaque certificat X509 v3, l'AC et le détenteur sont identifiés par un *Distinguished Name* (DN) de type X.509 v3.

- Les informations principales contenues dans les **certificats de l'AC racine et des AC émettrices** sont :

Champ de base	Valeur pour l'AC Racine	Valeur pour l'AC émettrice
Empreinte numérique	2f 09 30 d1 b4 ab 87 cb e6 52 0b 10 60 94 3 ^e 2d e8 4f 04 fb	2f 09 30 d1 b4 ab 87 cb e6 52 0b 10 60 94 3 ^e 2d e8 4f 04 fb
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Longueur des clés de l'AC	2048	2048
Key pair algorithm	RSA	RSA
Durée maximale avant l'expiration du certificat	20 ans	20 ans

- Les informations principales contenues dans **le certificat d'un détenteur** sont :

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC

	c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	User role; Certificate policies; Key usage; Mail.

Profil du certificat Signature niveau moyen avec OCSP

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.2 AIA = http://ocsp1.notarius.com/ocsp1-ccq (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl RFC822 = Email

Profil du certificat Signature niveau moyen-élevé avec OCSP

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA

Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.3 AIA = http://ocsp1.notarius.com/ocsp1-ccq (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl RFC822 = Email

Profil du certificat Signature et Encryption niveau moyen avec OCSP

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.2 AIA = http://ocsp1.notarius.com/ocsp1-ccq (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl RFC822 = Email

Champ de base	Valeur
---------------	--------

Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.5 Key usage = Chiffrement de la clé (2.5.29.15) CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl RFC822 = Email

Profil du certificat Signature et Encryption niveau moyen-élevé avec OCSP

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.3 AIA = http://ocsp1.notarius.com/ocsp1-ccq (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl

RFC822 = Email	
Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.6 Key usage = Chiffrement de la clé (2.5.29.15); CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl RFC822 = Email

Profil du certificat Signature et Encryption OAGQ

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
5Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.2 Key usage = Signature numérique (2.5.29.15); CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA

	CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl
	RFC822 = Email

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.5 Key usage = Chiffrement de la clé (2.5.29.15) CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl RFC822 = Email

Profil du certificat Signature Évaluation avec OCSP

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.1.0 AIA = http://ocsp1.notarius.com/ocsp1-ccq (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15);

	CPD = URL=ldap://x500a.notarius.net Adresse d'annuaire : CN=CRLx OU=AC1 O=CENTRE DE CERTIFICATION DU QUEBEC C=CA CPD = http://webcrl.notarius.net/crl/ccq_combined_crfile1.crl RFC822 = Email
--	--

7.2 Profil des LCR

Les LCR sont conformes à la norme X.509, version 3.

[LDAP://cn=CRL1,ou=AC1,o=CENTRE DE CERTIFICATION DU QUEBEC,c=CA](ldap://cn=CRL1,ou=AC1,o=CENTRE DE CERTIFICATION DU QUEBEC,c=CA)

Champ de base	Valeur
Émetteur	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Date d'entrée en vigueur	
Prochaine mise à jour	
Algorithme de signature	sha256RSA
Algorithme de hachage de la signature	sha256
Numéro de la liste de révocation des certificats	Nombres de CRL =00 ce 02
Identificateur de clé de l'autorité	Identifiant de la clé= 18 2f f3 b2 f2 62 92 2b 06 0d a9 d4 eb 53 2a 0f dd 0a 3f 03

7.3 Profil OCSP

Notarius propose la vérification du statut des certificats émis via des répondeurs OCSP (Online Certificate Status Protocol). Le répondeur OCSP permet de répondre en temps réel à des requêtes demandant le statut d'un certificat particulier sans avoir besoin de télécharger la LCR. L'OCSP de Notarius supporte le standard RFC 6960.

Les réponses OCSP contiennent des dates de validité permettant à l'utilisateur d'établir si la réponse OCSP est assez récente pour l'usage qu'il souhaite en faire.

Profil du certificat d'OCSP – CCQ

Champ de base	Valeur
Issuer DN	OU = AC1 O = CENTRE DE CERTIFICATION DU QUEBEC C = CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] serialnumber =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= CENTRE DE CERTIFICATION DU QUEBEC c=CA
Longueur des clés	2048
Durée de validité du certificat	10 ans
Durée de validité de la clé privé	2 ans
Extension du certificat	Certificate policies = 2.16.124.113550.1.3.2 : Cryptographic support required / Support cryptographique requis 2.16.124.113550.1.4.2 : Intended for server automation / Pour serveur automatisé Key Usager = Signature numérique (2.5.29.15) Extended Key usage = OCSP Signing (2.5.29.37) OCSP no revocation check (1.3.6.1.5.5.7.48.1.5)
CDP	http://webcrl.notarius.net/crl/ccq_combined_crlfile1.crl

7.4 Profil TSA

Non applicable.

8 Audit de conformité et autres évaluations

Les audits et les évaluations concernent non seulement ceux réalisés en vue de la délivrance d'une attestation de qualification au sens du règlement eIDAS, mais également ceux qui doivent être réalisés à la demande du PSC/R pour s'assurer que l'ensemble de l'ICP du CCQ est bien conforme aux engagements affichés dans la présente CP, dans la CPS et les politiques de sécurité afférentes, le tout pour s'assurer du respect des normes de sécurité en vigueur et du respect des lois et règlements applicables.

8.1 Fréquence et/ou circonstances des évaluations

Avant la première mise en service d'une composante clé de l'ICP du CCQ ou suite à une modification significative au sein d'une composante, le PSC/R procédera à un contrôle de conformité de cette composante.

Dans le cadre du programme d'audit du PSC/R, des audits internes et externes de certification et/ou de vérification sont effectués annuellement pour l'obtention et le maintien des accréditations eIDAS [ETSI EN 319 401, ETSI EN 319 411-1 & ETSI EN 319 411-2], ISO 27001 et ISO 9001.

8.2 Identités/Qualification des évaluateurs

Les contrôles sont effectués par des auditeurs compétents en sécurité des systèmes d'information ou dans le domaine d'activités de la composante contrôlée.

Les auditeurs désignés peuvent être internes comme externes au PSC/R.

Si un auditeur interne n'est pas en mesure de procéder à l'audit par manque de connaissance, il doit requérir les services d'un auditeur externe compétent en attendant de suivre une formation appropriée pour atteindre le niveau de connaissance requis.

Ces auditeurs se doivent d'être rigoureux pour s'assurer que les politiques, déclarations et services sont correctement mis en œuvre et détecter les cas de non-conformité qui pourraient compromettre la sécurité du service offert.

8.3 Relations entre évaluateurs et entités évaluées

Les auditeurs internes sont désignés par le PSC/R qui les autorise à contrôler les pratiques de la composante cible de l'audit.

Les auditeurs externes sont désignés par le PSC/R et doivent être indépendants et exempts de tout conflit d'intérêts de l'AC et du PSC/R.

8.4 Sujets couverts par les évaluations

Les auditeurs procèdent à des vérifications et des contrôles de conformité des services de certification offerts en se basant sur la Politique, la Déclaration des pratiques et les processus afférents.

Lors d'un audit externe, l'ampleur des sujets ou éléments à vérifier peut-être plus précise ou restreinte. L'auditeur établira un programme d'audit permettant de définir précisément quelle composante du service de certification est visée par l'audit.

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un audit, un rapport doit être produit par l'auditeur au PSC/R faisant état notamment des non-conformités et des opportunités d'amélioration. Il appartient au PSC/R de proposer un calendrier de résolution des non-conformités et des mesures à appliquer.

Dans toutes autres circonstances, un manquement peut être rapporté aux gestionnaires qui prendront les actions appropriées, le cas échéant.

8.6 Communications des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Frais d'abonnement ou d'utilisation

Des frais peuvent être exigés pour l'abonnement à un produit de l'ICP du CCQ ou son utilisation. Ces frais seront facturés selon l'échelle de tarifs diffusée par Notarius sur son site Web, ou négociée dans le cadre d'une entente particulière.

9.1.2 Frais d'accès aux LCR et à l'état des certificats

Lorsque le volume de vérifications est important ou que le service de vérification nécessite un niveau de service précis, des frais peuvent être exigés pour les tiers utilisateurs ayant besoin d'accéder aux LCR afin de vérifier l'état de validité des certificats des détenteurs.

À cet effet, une entente doit être conclue avec le PSC/R.

9.1.3 Frais pour la vérification de l'identité

- Les vérifications d'identité réalisées par l'AVI du PSC/R sont gratuites et exemptes de frais.
- Des frais discrétionnaires peuvent s'appliquer pour les vérifications d'identités réalisées par des notaires, répondants autorisés pour la vérification de l'identité des membres en règle de leur Ordre professionnel. Les frais chargés sont à la discrétion des répondants autorisés et le PSC/R n'a aucun contrôle sur ceux-ci.

9.1.4 Tarifs pour d'autres services

D'autres services pourraient être facturés. Dans ce cas, ces tarifs seront portés à la connaissance des personnes auxquelles ils s'appliquent.

9.1.5 Politique de remboursement

Dans le respect des conditions générales d'utilisation, tout certificat émis ne peut faire l'objet d'une demande de remboursement.

9.2 Responsabilité financière

Aucune limite n'est fixée dans la CP quant à la valeur d'une transaction dans le cadre de laquelle les certificats peuvent être utilisés. Cependant, le contrat d'utilisation peut limiter le type et la valeur des transactions pouvant être effectuées.

9.2.1 Couverture par les assurances

Les risques susceptibles d'engager la responsabilité de Notarius sont couverts par une assurance appropriée.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Le PSC/R possède une politique de confidentialité, disponible sur son site Web, indiquant le traitement qu'elle réserve aux renseignements qu'elle recueille, utilise, communique et conserve. Les informations suivantes détenues par le PSC/R sont considérées comme confidentielles (liste

non exhaustive) :

- Certains renseignements personnels relatifs au détenteur qui n'apparaissent pas dans les certificats;
- Les clés privées et les informations pour procéder à la gestion ou à la récupération d'un certificat ;
- Les registres de vérifications de l'ICP du CCQ;
- Les journaux d'évènements des composantes des AC;
- Les rapports d'audits;
- Le dossier d'enregistrement du client;
- Les enregistrements issus du processus de vérification de l'identité réalisé par l'AVI du PSC/R;
- Les causes de révocation, sauf accord explicite de publication;
- Les informations techniques relatives à la sécurité des fonctionnements de certaines composantes de l'ICP du CCQ et de son infrastructure.

9.3.2 Informations hors du périmètre des informations confidentielles

Les renseignements qui composent les certificats et le contenu des LCR ne sont pas considérés comme confidentiels.

9.3.3 Responsabilités en termes de protection des informations confidentielles

Toute collecte de données à caractère personnel par l'AC est réalisée dans le strict respect des lois et règlements en vigueur.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Tous les renseignements recueillis, utilisés, conservés ou communiqués dans le cadre de la prestation de services de certification sont assujettis à la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1). Notamment, toutes les informations recueillies dans le cadre de l'émission, de l'utilisation ou de la gestion des certificats ne doivent être utilisées ou communiquées que pour les fins pour lesquelles elles ont été recueillies.

Le PSC/R a implanté et maintient une politique de confidentialité accessible à tous et conforme aux lois applicables.

9.4.2 Informations à caractère personnel

Les renseignements personnels sont ceux qui permettent d'identifier une personne ou qui concernent une personne. Les données des dossiers d'enregistrement non publiées dans les certificats ou les LCR sont considérées comme confidentielles.

9.4.3 Informations à caractère non personnel

Pas d'engagement spécifique.

9.4.4 Responsabilité en termes de protection des données personnelles

Toute collecte de données à caractère personnel par l'AC est réalisée dans le strict respect des lois, règlements et politique en vigueur.

9.4.5 Notification et consentement d'utilisation des données personnelles

Les informations personnelles transmises à Notarius ne doivent ni être divulguées ni être transférées à un tiers, sauf dans les cas suivants : consentement préalable de la personne concernée, décision judiciaire ou autre autorisation légale.

En ce sens, l'AC respecte la Politique de confidentialité de Notarius.

9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Les enregistrements peuvent être mis à disposition en cas de besoin pour servir de preuve à la certification en justice, dans le respect de la Politique de confidentialité de Notarius.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Pas d'engagement spécifique.

9.5 Propriété intellectuelle

Solutions Notarius détient tous les droits de propriété intellectuelle sur la CP, la CPS, les applications et les infrastructures technologiques de l'ICP du CCQ, incluant le certificat racine de l'ICP du CCQ, les informations de révocation qu'elle émet & le nom de cette infrastructure, soit Centre de certification du Québec.

Les détenteurs détiennent tous les droits de propriété intellectuelle sur les renseignements qui leur sont personnels et qui apparaissent aux certificats émis par l'ICP du CCQ. Toutefois, le détenteur n'acquiert pas la propriété du certificat, mais seulement le droit d'usage.

Les applications utilisées en soutien à la prestation des services de certification ou celles utilisées par les détenteurs appartiennent à leurs fabricants respectifs. Ces derniers n'en confèrent qu'une licence d'utilisation lorsque les frais qui y sont reliés sont assumés.

9.6 Interprétations contractuelles et garanties

9.6.1 Relativement aux renseignements inscrits au certificat

Les renseignements contenus aux certificats et dont l'inscription est obligatoire doivent être conformes aux données vérifiées, en fonction du type de certificat demandé.

9.6.2 Relativement aux renseignements inscrits au répertoire

L'exactitude des LCR inscrite au répertoire doit être assurée.

9.7 Limite de garantie

À moins d'une entente contractuelle contraire, les limites de garantie sont exprimées dans les conditions générales d'utilisation de Notarius.

9.8 Limite de responsabilité

À moins d'une entente contractuelle contraire, les limites de responsabilité sont exprimées dans les conditions générales d'utilisation de Notarius.

9.9 Indemnisation

À moins d'une entente contractuelle contraire, en cas de reconnaissance d'une quelconque responsabilité de l'AC ou du PSC/R vis-à-vis d'un détenteur ou d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge, toutes causes confondues, sont limités à la plus petite valeur entre x) le montant prouvable des dommages réels directement subis par le client et y) la somme nette payée réellement par le client à Notarius pour les services applicables donnant lieu à toute telle réclamation, auxquels le client était abonné durant la période de 12 mois précédant tout dommage.

9.10 Procédures d'approbation

9.10.1 Approbation de la CP

Lorsque la CP est modifiée, elle doit être soumise pour approbation au Conseil d'administration de l'AC. Une fois les modifications approuvées, elle est publiée sur le site Web de l'AC dans un délai raisonnable et transmise aux ALE.

9.10.2 Approbation de la CPS

La CPS doit respecter les modifications approuvées de la CP.

Lorsque des modifications sont apportées à la CPS elles doivent être approuvées par le Comité de direction du PSC/R et l'AC doit en être avisée.

9.10.3 Durée de validité

La CP est valable jusqu'à ce qu'elle soit remplacée par une nouvelle version ou jusqu'à ce que l'AC cesse ses activités.

9.10.4 Applicabilité en cas d'invalidité

La fin de validité de la CP entraîne la cessation de toutes les obligations et responsabilités de l'AC et du PSC/R, sauf en ce qui a trait aux certificats émis sous son autorité qui sont toujours en vigueur, ceux-ci demeurent liés par les clauses de la CP.

9.11 Dispositions concernant la résolution des conflits

Les certificats émis en vertu de la présente CP sont des certificats dont les conditions d'utilisation sont définies par la présente CP et par les conditions générales d'utilisation qui définissent les relations entre Notarius et les utilisateurs finaux.

9.12 Juridictions compétentes

Tout conflit découlant des services de l'ICP du CCQ doit être prioritairement réglé par la négociation.

Si cela s'avère impossible ou infructueux, un médiateur indépendant est mandaté, après

acceptation par les parties.

En cas d'échec de la médiation, tout litige relatif à la validité, l'interprétation, l'exécution de la présente CP sera soumis aux tribunaux du district judiciaire de Montréal, province de Québec. L'application de la Convention des Nations unies sur les contrats de vente internationale de marchandise est expressément exclue.

9.13 Interprétation

9.13.1 Lois et règlements applicables

La présente CP est régie et interprétée en vertu des lois, des règlements, des directives et des normes applicables au Québec et au Canada.

9.13.2 Indépendance des dispositions

Le fait pour une ou plusieurs dispositions de la CP d'être déclarées invalides, illégales ou inapplicables ne porte pas atteinte à la validité des autres dispositions.

La CP continuera donc à s'appliquer en l'absence de la disposition inapplicable.

9.14 Revue

La CP du CCQ sera revu annuellement.

9.15 Entrée en vigueur

La CP entre en vigueur à la date d'adoption par le Conseil d'administration de Solutions Notarius Inc.