notarius
UNE ENTREPRISE PORTAGE CYBERTECH

Diffusion publique

DÉCLARATION DES PRATIQUES DE CERTIFICATION

LES ICP DE NOTARIUS[MD]

Version : 4.1
OID : 2.16.124.113550.2
Date d'approbation : 2025-11-27

Notes aux lecteurs

Un changement a été apporté à la présente version de la Déclaration des pratiques de certification des ICP de Notarius, soit :

- Révision pour conformité Mozilla / CA/B.

Suivi des versions

Version	Date	Description	Rédacteurs	Approbateur
1.2	2015/05/26	Version initiale	Liette Boulay, Directrice Services juridiques et conformité	Comité de direction de Solutions Notarius Inc.
1.3	2017-02-17	Version revue pour satisfaire les exigences de WebTrust	Maud Soulard, Officier ICP	Comité de direction de Solutions Notarius Inc.
2.0	2017-12-14	Modifications pour conformité à la norme eIDAS	Maud Soulard, Officier ICP Alexandre Provost, Chef d'équipe TI	Comité de direction de Solutions Notarius Inc.
3.0	2019-12-16	Mise à jour suite à l'audit de qualification eIDAS Précision des processus liés aux produits CertifiO Organisation et CertifiO Département Ajout d'ICA3 et du CEV	Maud Soulard, Officier ICP	Comité de direction de Solutions Notarius Inc.
3.1	2019-12-19	Mise à jour suite à l'audit eIDAS en conformité avec le contrôle CCS-6.3.10-13 de ETSI EN 319 411-2	Maud Soulard, Officier ICP	Comité de direction de Solutions Notarius Inc.
3.2	2020-10-26	Confirmation de la validation du courriel du détenteur	Maud Soulard, Officier ICP	Comité de direction de Solutions Notarius Inc.
3.3	2021-11-24	Ajout des nouvelles empreinte numériques	Maud Soulard, Officier ICP	Comité de direction de

				Solutions Notarius Inc.
3.4	2022-11-15	Modifications pour conformité à la norme eIDAS	Maud Soulard, Officier ICP Alexandre Provost, Chef de la sécurité	Comité de direction de Solutions Notarius Inc.
4.0	2025-11-21	Refont de la table des matières – Conformité Mozilla	Maud Soulard, Officier ICP	Comité ISO+ de Solutions Notarius inc.
4.1	2025-11-27	Correction ECC P-256	Maud Soulard, Officier ICP	Comité ISO+ de Solutions Notarius inc.

Propriété intellectuelle

Table des matières

1 Dispositions générales

1.1 Présentation générale

Solutions Notarius[MD] 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.
Notarius propose également à ses clients une solution de sécurisation des documents par code à barre, le cachet électronique visible (CEV), qui comprend les données clés signées électroniquement permettant de détecter toute altération et de confirmer l'authenticité et la légitimité de l'émetteur[1].
Notarius est également prestataire de service de certification depuis plusieurs années auprès des professionnels et de leurs partenaires d'affaires.
Notarius est la seule entreprise au Canada à certifier des identités de confiance et d'affiliations professionnelles émettant des signatures numériques de confiance reconnues aussi bien par Adobe que Microsoft.

Les infrastructures à clés publiques (ICP) de Notarius autorisent non seulement l'émission des clés et certificats permettant de signer des documents électroniques, mais également d'en encapsuler les données clés.
On peut donc dire que :

- La signature numérique de Notarius 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.
- L'encapsulage garantit l'origine et l'intégrité des données clés des documents.

La présente Déclaration des pratiques de certification (CPS) décrit les procédures et les exigences appliquées par le Prestataire de service de certification et de répertoire (PSC/R) pour émettre et gérer les signatures numériques qualifiées et avancées et les cachets électroniques visibles (CEV) de l'ICP dans le respect de la Politique de Certification (CP).
La CPS décrit donc non seulement la gestion du service et la gestion de l'infrastructure, le fonctionnement et les procédures de création, de délivrance, de gestion et d'utilisation de certificats, mais également les exigences relatives à la vérification de l'identité des détenteurs et les intervenants impliqués.

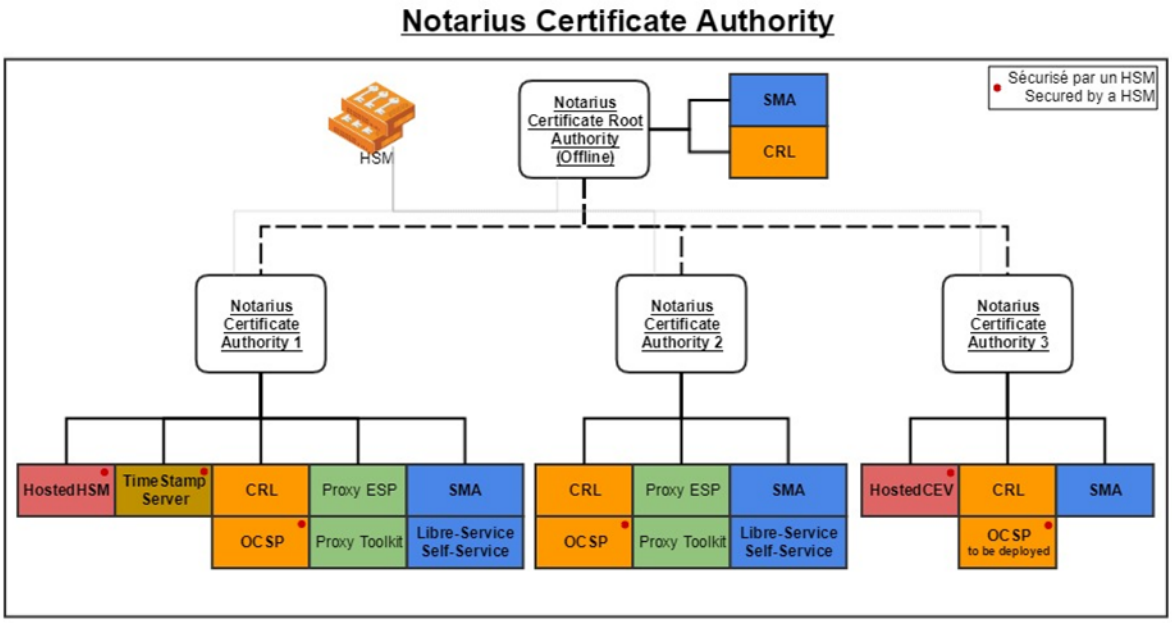
Cette CPS est conforme aux principes et recommandations définis dans les normes ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 & ETSI EN 319 412-3.
La présente CPS répond également aux standards et recommandations de l'AIGCEV pour l'émission des CEV.

La présente Déclaration des pratiques de certification suit strictement la structure et la numérotation prescrites par le RFC 3647 et couvre l'ensemble des pratiques

[1] *https://otentik.codes/fr/*

opérationnelles mises en œuvre par Notarius en tant qu'Autorité de certification

Comme Notarius est détenteur de plusieurs ICP, le périmètre de la présente CPS ne se limite qu'aux ICP de Notarius communément appelées ICA1, ICA2 et ICA3 (voir schéma ci-dessous).



1.2 Identification du document (OID)

La présente CPS doit être lue conjointement avec les Politiques de certification (CP) applicables aux différentes ICP de Notarius. La CP établit les exigences de haut niveau ; la CPS décrit la manière dont ces exigences sont mises en œuvre.
L'identificateur d'objet (OID) de la Déclaration des pratiques de certification de Notarius est : 2.16.124.113550.2

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

Description	Identificateur d'objet (OID)
Certificat de l'AC Racine : *Notarius Root Certification Authority*	**2.16.124.113550.2.1**
Certificat de l'AC émettrice : Notarius Certificate Authority	**2.16.124.113550.2.2**
• Niveau d'assurance de l'identité	2.16.124.113550.2.2.1
○ Identity NOT verified / Identité NON vérifiée ***Certificat de test/démo***	2.16.124.113550.2.2.1.0
○ Identity verified face-to-face / Identité vérifiée en	2.16.124.113550.2.2.1.1

face-à-face	
• Nature d'identités certifiées	2.16.124.113550.2.2.2
○ Natural person / Identité d'un individu physique	2.16.124.113550.2.2.2.1
○ Legal person / Personne morale	2.16.124.113550.2.2.2.2
• Support minimum requis	2.16.124.113550.2.2.3
○ Software support / Support logiciel	2.16.124.113550.2.2.3.1
○ Cryptographic support required / Support cryptographique requis	2.16.124.113550.2.2.3.2
• Fonctions spécifiques	2.16.124.113550.2.2.4
○ Intended for server automation / Pour serveur automatisé	2.16.124.113550.2.2.4.1
○ Complies with Adobe Approved Trust List (AATL) / Conforme à Adobe Approved Trust List (AATL) ***Reconnaissance AATL***	2.16.124.113550.2.2.4.2
○ Certificat généré et géré par Notarius au nom du détenteur / Certificate generated and managed by Notarius on behalf of the holder. ***Remote QSCD***	2.16.124.113550.2.2.4.3
Certificat de l'AC émettrice 2 : Notarius Certificate Authority 2	**2.16.124.113550.2.3**
▪ Niveau d'assurance de l'identité	2.16.124.113550.2.3.1
○ Identity NOT verified / Identité NON vérifiée ***Certificat de test / Démo***	2.16.124.113550.2.3.1.0
○ Identity verified face-to-face / Identité vérifiée en face-à-face	2.16.124.113550.2.3.1.1
▪ Nature d'identités certifiées	2.16.124.113550.2.3.2
○ Natural person / Identité d'un individu physique	2.16.124.113550.2.3.2.1
○ Legal person / Personne morale	2.16.124.113550.2.3.2.2
▪ Support minimum requis	2.16.124.113550.2.3.3
○ Software support / Support logiciel	2.16.124.113550.2.3.3.1
○ Cryptographic support required / Support cryptographique requis	2.16.124.113550.2.3.3.2
▪ Fonctions spécifiques	2.16.124.113550.2.3.4
○ Intended for server automation / Pour serveur automatisé	2.16.124.113550.2.3.4.1
Certificat de l'AC émettrice 3 : Notarius Certificate Authority 3	2.16.124.113550.2.4
▪ Niveau d'assurance de l'identité	2.16.124.113550.2.4.1
○ Identity NOT verified / Identité NON vérifiée ***Certificat de test/Démo***	2.16.124.113550.2.4.1.0

○ Identity verified face-to-face / Identité vérifiée	2.16.124.113550.2.4.1.1
▪ Nature d'identités certifiées	2.16.124.113550.2.4.2
○ Natural person / Identité d'un individu physique	2.16.124.113550.2.4.2.1
○ Legal person / Personne morale	2.16.124.113550.2.4.2.2
▪ Support minimum requis	2.16.124.113550.2.4.3
○ Software support / Support logiciel	2.16.124.113550.2.4.3.1
○ Cryptographic support required / Support cryptographique requis	2.16.124.113550.2.4.3.2
▪ Fonctions spécifiques	2.16.124.113550.2.4.4
○ Intended for server automation / Pour serveur automatisé	2.16.124.113550.2.4.4.1
Autres OID et sous-structures utilisées	
AIGCEV	
▪ Racine	1.3.6.1.4.1.51528
▪ Security	1.3.6.1.4.1.51528.1
○ UsageList	1.3.6.1.4.1.51528.1.1
○ Trusted Timestamp	1.3.6.1.4.1.52528.1.2
▪ Certification Practise Statement – CPS A sequence of UUIDs	1.3.6.1.4.1.51528.2
▪ Test Certificate The identity and legitimacy of the issuer HAS NOT BEEN VERIFIED and MUST NOT BE TRUSTED	1.3.6.1.4.1.51528.2.1
Adobe	1.2.840.113583
▪ Acrobat	1.2.840.113583
▪ Acrobat Security	1.2.840.113583.1
▪ pdfX509Extension	1.2.840.113583.1.9
○ pdfTimestamp ***URL TSA personnalisé***	1.2.840.113583.1.9.1
▪ Adobe CPS OIQ	1.2.840.113583.1.2
▪ Intended for Adobe / Pour test Adobe ***certificat de test***	1.2.840.113583.1.2.2
IANA *(Internet Assigned Numbers Authority)*	
▪ Iana Security-related objects	1.3.6.1.5
▪ Mechanisms	1.3.6.1.5.5
▪ PKIX	1.3.6.1.5.5.7

▪ Private certificate extensions	1.3.6.1.5.5.7.1
○ AuthorityInfoAccess (AIA) *URL OCSP*	1.3.6.1.5.5.7.1.1
▪ Extended key purpose OIDS	1.3.6.1.5.5.7.3
○ Timestamping	1.3.6.1.5.5.7.3.8
○ OCSP Signing	1.3.6.1.5.5.7.3.9
▪ Access descriptors	1.3.6.1.5.5.7.48
○ OCSP	1.3.6.1.5.5.7.48.1
○ OCSP-nocheck	1.3.6.1.5.5.7.48.1.5
Exemple d'OID utilisés conformément aux requis eIDAS	
ETSI 411-2	
▪ EU qualified certificates issued to a natural person (QCP-n), with the policy identifier OID 0.4.0.194112.1.0 (QCP-n)	0.4.0.194112.1.0
▪ EU qualified certificates issued to a legal person (QCP-l), with the policy identifier OID 0.4.0.194112.1.1 (QCP-l)	0.4.0.194112.1.1
▪ EU qualified certificates and requiring the use of a Qualified Signature Creation Device (QSCD) issued to natural person QCP-n-qscd (non-repudiation)	0.4.0.194112.1.2
▪ EU qualified certificates and requiring the use of a Qualified Signature Creation Device (QSCD) issued to legal person QCP-l-qscd (digital signature)	0.4.0.194112.1.3

1.3 Définitions et abréviations

1.3.1 Abréviations

- **AATL**: Adobe Approved Trust List
- **AC** : Autorité de certification
- **AIGCEV** : Association Internationale de Gouvernance du Cachet Électronique Visible
- **ALE** : Autorité locale d'enregistrement
- **ANS :** Accords sur les niveaux de services
- **AVA** : Agent de vérification de l'affiliation
- **AVI** : Agent de vérification de l'identité
- **CEV** : Cachet Électronique Visible
- **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
- **FIPS :** *Federal Information Processing Standard*
- **HSM** : *Hardware Security Module*
- **ICP** : Infrastructure à clés publiques
- **ISO** : International Standard Organization
- **LAR** : Liste des autorités révoquées
- **LCR** : Liste des certificats révoqués
- **LS** : Potail client « Mon compte Notarius »
- **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
- **RTO** : Objectif de délai de reprise
- **RPO** : Perte maximale de données

1.3.2 Définitions

Les termes utilisés dans la CPS sont les suivants :

- **Abonnement** : l'abonnement souscrit par le Détenteur ou l'Acheteur, selon le cas applicable, à l'un ou plusieurs produits de Notarius.
- **Acheteur** : personne qui initie le processus d'abonnement à l'un des produits de Notarius pour elle-même ou pour un détenteur autorisé.
- **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. 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 le mot de passe de son certificat de signature numérique, de modifier le mot de passe de son Compte Notarius, d'effectuer certaines opérations de configuration ou de réaliser des transactions au moyen de ses certificats.
- **Application de vérification du CEV** : L'application mise en œuvre par l'utilisateur pour vérifier le CEV des données reçues à partir de la clé publique du serveur contenue dans le certificat.
- **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.
- **Cachet Électronique Visible (CEV)** : dispositif qui garantit l'origine et l'intégrité des données clés d'un document et qui, pour ce faire, encapsule les données accompagnées de leur signature numérique pour organisation (ou départementale) dans un code à deux (2) dimensions. Le CEV auquel réfère la présente CP est le ***CEV Otentik***, dont la gouvernance est dictée par l'AIGCEV.
- **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. Cet ensemble d'informations atteste qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié dans le certificat. Le certificat est valide pendant une durée donnée précisée dans celui-ci.
- **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 personne physique ayant adhéré au service (par lui-même ou par un acheteur) et qui détient des clés et des certificats de l'ICP lui permettant de signer, s'authentifier et/ou chiffrer selon ses besoins ou les fonctionnalités disponibles. Le Détenteur est un utilisateur final dûment autorisé de l'un des produits de Notarius; il peut être titulaire d'un certificat qui sera affecté soit à un groupe, soit à 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.
- **Entiercement** : ou « escrow agreement » consiste pour un fournisseur d'un produit ou d'un service, à confier à un tiers séquestre des éléments essentiels (logiciels, bases de données, documents, etc.) à l'usage de ce produit ou à la réalisation de ce service. L'objectif est d'assurer à un tiers (client, partenaire, etc.) la possibilité d'y accéder, selon les dispositions prévues entre les parties, et notamment en cas de défaillance du fournisseur.
- **Frais d'Abonnement** : les frais d'Abonnement que l'Acheteur doit payer annuellement ou mensuellement, selon le cas, pour l'utilisation par un Détenteur d'un ou plusieurs Produits, en sus des Frais d'adhésion et des Frais transactionnels.
- **HSM** : Boîtier cryptographique matériel dans lequel sont stockés les clés publiques et privées des autorités de certification.
- **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.
- **Information personnelle** : toute information ou tout renseignement de nature personnelle qui concerne un individu et qui permet de l'identifier. Les Informations personnelles recueillies par Notarius afin d'assurer que les certificats de signatures numériques émis sont valides et fiables peuvent contenir les prénoms et les noms de famille, les coordonnées et des photocopies de preuves d'identité valides émises par le gouvernement à des fins d'identification. La collecte, la conservation, l'utilisation, la divulgation et la destruction de ces informations sont effectuées conformément aux lois et règlements applicables en matière de protection des renseignements personnels, incluant les lois protégeant les renseignements personnels du Québec et les politiques de certification de Notarius ainsi qu'à la Politique de confidentialité de Notarius. Les Informations personnelles conservées

par Notarius sont chiffrées localement, protégées contre les pirates informatiques et protégées contre les pertes de données de même que l'utilisation interne non autorisée. Les Informations personnelles peuvent seulement être consultées par des Officiers spécifiques de Notarius dans des circonstances particulières telles qu'un doute sur la validité de l'émission d'un certificat numérique ou une ordonnance d'un tribunal ou d'une ordonnance de divulgation des renseignements personnels.

- **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.
- **« Mon Compte »** : Le compte Notarius est un compte en ligne sécurisé (nom d'usager / mot de passe) permettant au Détenteur un accès sécurisé à différents Produits offerts par Notarius (ex : portail administratif Mon Compte, Signature CertifiO Cloud). En outre, Mon Compte comporte certaines fonctionnalités pour la gestion du cycle de vie du certificat de signature numérique du Détenteur
- **Objectif de délai de reprise (RTO)** : durée après un incident pendant laquelle un produit ou service ou une activité est reprise, ou des ressources sont rétablies. Pour les produits, les services et les activités, l'objectif de délai de reprise est inférieur au temps qu'il faudrait pour que les impacts défavorables qui résulteraient du défaut de fourniture d'un produit/service ou de l'absence de réalisation d'une activité, deviennent inacceptables.
- **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.
- **Perte maximale de données:** aussi identifié comme point de récupération des données **(RPO)** est le point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre son fonctionnement à la reprise.
- **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.

- **Processus d'approbation et de révocation automatisé** : Service permettant l'automatisation par un Ordre professionnel de l'étape d'approbation des demandes d'adhésion à la signature numérique pour professionnel de ses membres ou encore la révocation de celle-ci fondé sur la transmission et le traitement des données directement issues du tableau de l'Ordre fournies sur une base quotidienne à Notarius.
- **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.
- **Signature numérique** : les clés privées et publiques contenues dans un certificat émis à un Détenteur dans le but de l'identifier dans le cadre de son utilisation des Produits. Les certificats comprennent l'ensemble des renseignements confirmant l'identité d'un Détenteur. Notarius lie de manière cryptographique une identité officielle au certificat de Signature numérique protégé par une authentification à deux facteurs qui est délivré de manière sécurisée à un utilisateur validé. Les Signatures numériques émises par Notarius peuvent être apposées sur les documents PDF, PDF/A et tout autre type de documents supportés. Les types de Signatures numériques varient selon le(s) Produit(s) souscrit(s). Une Signature numérique demeure valide tant et aussi longtemps qu'elle n'est pas expirée ou révoquée.
- **Tiers utilisateur** : Personnes agissant en se fiant à un certificat émis par l'ICP. Il peut être ou non lui-même un détenteur de certificats de l'ICP.

1.4 Interprétation

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

1.5 Conformité aux normes applicables

Les pratiques mentionnées dans le présent document sont détaillées notamment dans le but de satisfaire les exigences de l'industrie en la matière.

Ces pratiques définissent les engagements de Notarius dans le cadre de la fourniture de certificats qualifiés et avancés en conformité avec les normes ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 & ETSI EN 319 412-3.
La structure de la CPS se calque sur celle du RFC 3647 (*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*[2]) aux fins de meilleure compréhension.

1.6 Les composantes de l'ICP

1.6.1 L'autorité de certification (AC)

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

- Délivrer des certificats dans le respect de la CPS et de la CP;
- Adopter ou modifier la CP;
- Choisir 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 ;
- Publier la liste des certificats révoqués (LCR) et de celle des autorités révoquées (LAR).

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

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

Le Comité de direction de Notarius est composé du Président et chef de la direction de Notarius, de la vice-présidente finances et administration (également Officier ICP), du vice-président ventes et développement des affaires 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, incluant les Officiers ICP;
- Des aspects administratifs et technologiques associés à la délivrance des certificats comme la validation de l'identité et de la qualité des détenteurs ou encore la conservation sécuritaire des pièces au dossier;
- Des opérations subséquentes reliées au cycle de vie des certificats ;

[2] *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)*

- 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 ;
- De s'assurer que l'AC publie bien les LCR, les LAR ainsi que les certificats publics des détenteurs ;
- 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 les moyens nécessaires et conformes aux meilleures pratiques pour assurer la sécurité des services de répertoire ;
- D'assurer la conservation des 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 (voir l'extrait du Procès-verbal du CA du 25 février 2015 : CA-2015-1-10.1 Affaires diverses).

- Les ententes contractuelles signées sont classées dans des répertoires dédiés à accès restreints.
- Les versions originales papier, lorsqu'elles existent, sont classées dans une voûte (classeur noir ignifuge) à accès restreint proche du bureau de la vice-présidente finances et administration.

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. Les AVA doivent également compléter les formulaires d'engagement le cas échéant :

- AVA corporatif (est identifié dans le formulaire d'ouverture de compte) :
- AVA corporatif
- AVA professionnel - nomination
- AVA professionnel - engagement

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 ;
- Pour chaque jour ouvrable, s'assurer qu'au moins un (1) AVA est disponible, formé et prêt à approuver ou révoquer les signatures numériques des employés ou membres de l'ALE ou pour traiter des exceptions à la vérification automatisée du statut du membres dans les cas où l'ALE est un Ordre professionnel qui a adhéré à l'automatisation des approbations et des révocations;
- S'assurer que les AVA respectent les obligations identifiées dans la CP ou toute entente contractuelle particulière;
- S'assurer que les informations du tableau de l'Ordre professionnel (ou Registre des membres) soient toujours à jour et exempt d'erreur lorsqu'il a décidé d'adhérer au Processus d'approbation et de révocation automatisé.

L'ALE ou son AVA :

- Appliquent et respectent la CP, la CPS, les ententes contractuelles signées et les procédures d'utilisation du Portail de gestion, lorsqu'applicable ;
- Approuvent ou rejettent l'enregistrement des demandes initiales de certificats qui leur 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 dans un délai maximal de 24 heures entre la réception de la demande de révocation et la décision de modifier l'information sur l'état de cette demande ;
- Demandent au PSC/R de procéder à la révocation des signatures numériques corporatives de ses employées portées à son compte corporatif;
- À moins d'entente contractuelle contraire, est le support de 1er 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 est une personne physique ou une entité/un groupe/une application (par exemple dans le cadre des certificats pour département ou pour organisation) qui utilise son certificat pour signer, pour s'authentifier et/ou pour chiffrer

selon ses besoins ou les fonctionnalités qui lui sont disponibles.
Le détenteur est un utilisateur final dûment autorisé de l'un des produits de Notarius.

1.6.4.2 Rôles et responsabilités

Comme l'utilisation de la signature numérique CertifiO pour employés ou CertifiO pour professionnels est un droit personnel et qu'il est strictement interdit de confier ou encore de divulguer à quiconque les informations permettant de l'utiliser. Également, comme l'utilisation de la signature numérique CertifiO pour départements ou CertifiO pour organisation est un droit personnel, il est strictement interdit de confier ou encore de divulguer à quiconque n'étant pas autorisé à l'intérieur du département ou de l'organisation identifiée les informations permettant d'utiliser cette signature sous peine de révocation immédiate.

En tout temps, le détenteur doit :

- Respecter les conditions qui lui incombent telles que définies dans la CP et la CPS;
- Respecter les conditions générales ou particulières d'utilisation des produits de Notarius disponibles en tout temps sur son site web;
- Remplir les obligations relatives à son adhésion telles que requises par le PSC/R, notamment en suivant les étapes d'adhésion du produit sélectionné, disponible en tout temps sur le site Web de Notarius.
- Fournir les informations, pièces et documents requis par le PSC/R, notamment celles qui apparaissent dans les propriétés de la signature numérique comme son nom, son prénom, son numéro de membre (lorsqu'applicable), son adresse de courriel professionnel ;
- Protéger 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 de compte et mot de passe de signature. ;
- S'assurer qu'il est le seul à utiliser ses certificats (par exemple, ne jamais confier ses certificats à un collègue ou une collaboratrice) 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 ;
- Utiliser ses certificats pour les seules fins autorisées ;
- Signer en ligne ses documents pour en assurer l'authenticité ;
- Utiliser son équipement informatique de façon sécuritaire, notamment en fermant sa session de signature numérique avant de quitter son poste ;
- Aviser dans les meilleurs délais le service à la clientèle du PSC/R au 1-855-505-7272 s'il soupçonne que la confidentialité de ses clés et certificats, ou du mot de passe de son certificat de signature numérique ou celui de son compte, sont compromis ;
- Informer le plus rapidement possible le PSC/R de tout changement ou procède lui-même aux changements requis via le portail client "Mon compte Notarius", notamment quant à son adresse courriel ou à ses coordonnées ;
- Arrêter d'utiliser ses certificats lorsqu'ils 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 transige de façon électronique avec des détenteurs de certificats.
Il est autorisé et a conclu une entente contractuelle formelle 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 de l'ICP ;
- 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 ;
- D'effectuer la gestion des accès et des autorisations à ses applications informatiques ;
- D'effectuer les mises à jour requises pour suivre l'évolution de l'ICP ;
- 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 aura préalablement déterminés.

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.
Il peut être ou non lui-même un détenteur de clés et de certificats de l'ICP.
Le tiers utilisateur souhaitant agir en se fondant sur un certificat doit s'assurer que ce certificat :

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

Le tiers utilisateur souhaitant agir en se fondant sur un CEV doit également s'assurer que le signataire avait la légitimité de signer le cas d'usage. Pour ce faire, le tiers utilisateur se fondera sur l'extension « PracticeStatement » du cas d'usage qui décrira le processus requis en valider la légitimité.

Le tiers utilisateur peut vérifier la fiabilité des documents électroniques PDF signés à l'aide de la signature numérique CertifiO[MD] ou par la plateforme de signature électronique ConsignO Cloud[MD] ou encore vérifier la fiabilité des documents imprimés qui disposent d'un CEV CertifiO[MD] Code en utilisant VerifiO[MD].

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 présente CPS 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 ;
- Chiffrer des documents électroniques afin d'assurer la confidentialité de l'information, si applicable;
- Signer les données contenues dans le CEV Otentik.

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 CPS.

Le tableau suivant fournit une brève description des utilisations appropriées des signatures numériques de la gamme CertifiO[MD]. 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. 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. Certifie également le nom de l'employeur.
CertifiO pour départements	Certificat de signature numérique, certifiant le nom du département ou de l'organisation et associant le document signé au département ou à l'organisation. Certifie l'authenticité du document émis par le département ou l'organisation.

	La signature est réalisée par un employé au nom de l'organisation, pour un maximum de 2 000 signatures annuellement. Délivré sur un jeton de sécurité USB émis par Notarius. Reconnu par les produits d'Adobe sans aucune modification à leur configuration. Ces certificats peuvent aussi être délivrés soft-token.
CertifiO pour organisations	Certificat de signature numérique, certifiant le nom du département ou de l'organisation, et associant le document signé au département ou à l'organisation. Pour utilisation par un serveur, généralement pour de grands volumes de documents signés annuellement. Délivré par son service de Hosted HSM ou sur des jetons de sécurité USB émis par Notarius. Reconnu par les produits d'Adobe sans aucune modification à leur configuration.
CertifiO Code	Certificat de signature numérique signant le cachet électronique visible afin d'en assurer l'intégrité et l'authenticité. Délivré pour un ou des cas d'usage spécifiques tel qu'autorisés par l'AIGCEV. Est émis à un organisme généralement responsable de l'émission des documents sur lesquels le CEV sera apposé.
CertifiO pour évaluation	Certificat de signature numérique pour évaluation uniquement. Ne certifie **pas** l'identité, le statut professionnel ou le lien d'emploi. Le certificat inclut une métadonnée indiquant à Adobe Acrobat et à ConsignO que l'identité du signataire n'a pas été vérifiée et n'est donc pas fiable.

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 des produits de Notarius, les accords sur le niveau de service ou les spécifications d'un produit peuvent limiter les utilisations que peut faire le détenteur de ses certificats, incluant le nombre d'utilisations. Tous les produits offerts par Notarius sont limités à une utilisation raisonnable et non-abusive qui varie selon la spécification du service. À titre d'exemple et sans en limiter la portée, l'utilisation de CertifiO pour processionnels, pour Employés et pour Départements est réservée aux signataires ayant pris connaissance spécifique des documents à signer, que ce soit à l'unité ou en lot; également l'utilisation de CertifiO pour organisations est limitée aux nombres de signatures spécifiées dans l'abonnement.
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.
Également, les détenteurs s'engagent à ne plus utiliser leur certificat dès la révocation ou l'expiration de celui-ci.

Enfin, toute utilisation non spécifiée dans la présente CPS est strictement interdite.
Notarius ne peut en aucun cas être tenu responsable de l'utilisation des certificats émis selon cette CPS à des fins et selon des modalités autres que celles qui y sont expressément prévues.

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 ;
- Un individu agissant pour une Personne morale (employé, mandataire, etc.) dont les clés et les certificats seront affectés à un groupe, un dispositif ou une application ;
- Toute personne physique qui désire un certificat pour ses propres besoins et qui répond aux exigences du PSC/R.

1.8 Gestion de la CPS

1.8.1 Responsable de la CPS

La CPS est sous la responsabilité de Notarius.

1.8.2 Coordonnées du responsable

Pour toute question ou remarque concernant la CPS, les certificats émis 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 CPS et de la CP

Notarius via son CEO approuve la CP.
Notarius via son Comité ISO+ 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 ISO+ de Notarius, pour donner suite à la révision de la CPS par l'Officier ICP et l'arrimage aux changements de la CP approuvés par le CEO de Notarius.

Toute mise à jour de la CPS suivra le processus d'approbation mis en place et sera publiée sur le site Web de Notarius dans les deux langues officielles.

2 Publication et diffusion de l'information

Notarius maintient un répertoire d'information public contenant l'ensemble des documents et données nécessaires pour permettre aux abonnés, aux parties de confiance et aux auditeurs de vérifier les pratiques de l'Autorité de certification et le statut des certificats émis. Toutes les informations publiées par Notarius sont accessibles librement, sans exigence d'authentification, de création de compte, de cookies ou de mécanismes restrictifs d'accès

Le PSC/R a la charge de la mise à disposition et de la publication via son site Web de la CP, de la CPS, des conditions générales et particulières d'utilisation de ses produits ainsi que de ses RTO et RPO via ses ANS.
Il met également à disposition des utilisateurs et des applications utilisatrices des certificats qu'il émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC.

Le PSC/R est donc responsable de la publication et de la diffusion des informations, en fonction des exigences de disponibilité. Par exemple :

- Le répertoire où sont publiées les LCR et l'information des certificats sont accessibles en ligne en tout temps pour les détenteurs, les tiers utilisateurs et tout autre intervenant faisant partie de l'ICP, sauf lors d'une maintenance ou en cas de force majeure.
- Le répertoire des certificats est accessible selon le niveau de service défini par le PSC/R.
    - L'accès est sans frais, lorsque réalisé par un individu qui effectue un faible nombre de requêtes quotidiennement. Dans tous les autres cas, l'accès nécessite une entente avec le PSC/R.
    - Les inscriptions apparaissant aux répertoires de l'ICP sont utilisées par les détenteurs ou les tiers utilisateurs seulement pour accéder au certificat de chiffrement public d'un détenteur et pour accéder aux LCR et LAR.

Tous les documents et informations publiés par Notarius sont accessibles librement au public, sans aucune exigence d'authentification, de création de compte, d'identification préalable ou de mécanisme de contrôle d'accès. Les CRL et les réponses OCSP ne requièrent aucun cookie, aucune session et aucun mécanisme de suivi.

Les informations diffusées publiquement sur le site Web du PSC/R pour l'AC sont :

- Les Politiques de certification (CP) applicables aux différentes infrastructures de clés publiques opérées par Notarius;
- La présente CPS
- Les conditions générales et particulières d'utilisation de ses produits
- Les accords sur le niveau de services incluant ses RPO et RTO (ANS)
- La politique de confidentialité
- Le Code d'Éthique et de conduite
- Les formulaires de demande de certificat

- Le certificat de l'AC racine Notarius Root Authority;
- Les certificats des Autorités de certification émettrices (Notarius Certificate Authority et variantes numérotées);
- Les Listes de révocation de certificats (CRL/LCR) à jour et signées:
- La Liste d'Autorité de révocation (LAR) associée à l'AC racine.
- Les points de publication OCSP, tels que définis dans les profils de certificats (voir section 7)

2.1 Points de distribution CRL et OCSP

Les CRL de toutes les AC exploitées par Notarius sont publiées et mises à jour conformément aux exigences des profils de certificats et des normes applicables.
Les CRL listées ci-dessous sont accessibles librement :

- http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl
- http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl
- http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl
- http://crl1.notarius.com/crl1-ca3/crl/notarius_certificate_authority_3_crlfull.crl

Liste d'autorité de révocation (LAR) :

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

Les services OCSP (*Online Certificate Status Protocol*) permettant la vérification en temps réel du statut des certificats sont également publiés dans le répertoire d'information public. Les URL OCSP spécifiques à chaque AC sont indiquées dans les profils de certificats (section 7).
Ces points d'accès OCSP sont disponibles 24 heures sur 24, 7 jours sur 7, sans authentification ni condition d'accès, conformément aux exigences du CA/Browser Forum et de Mozilla.

2.2 Fréquence des publications

Les informations liées à l'ICP de Notarius 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 est diffusé préalablement à toute diffusion des LCR correspondantes.
- La ***LCR*** est mise à jour et diffusée au moins toutes les deux (2) heures et publication immédiate en cas de révocation urgente.
- La durée de validité de la ***LCR*** est d'un maximum de quarante-huit (48) heures.

- ***Services OCSP*** : disponibilité continue (24/7) avec une mise à jour des statuts conforme aux exigences des normes ETSI et des CA/Browser Forum.
- Les ***CP*** est publiées sur le site Web de Notarius dans les meilleurs délais suivant leur adoption par le CEO de Notarius. Elles sont donc disponibles 24h/24 et 7j/7.
    - Le détail des mises à jour apportées à la CP sont clairement identifiées à la section notes aux lecteurs et historique des versions de ladite CP.
    - Si applicable, les changements apportés à la CP susceptibles d'affecter l'acceptation du service par les professionnels leur seront notifiés par courriel dans le respect des ententes contractuelles en place ou directement sur le site Web du PSC/R.
- La **CPS** est publiée sur le site web de Notarius dans les meilleurs délais suivant son adoption par le Comité de direction de Notarius. Elle est donc disponible 24h/24 et 7j/7.
    - Le détail des mises à jour apportées à la CPS sont clairement identifiées à la section notes aux lecteurs et historique des versions de ladite CPS.
    - Si applicable, les changements apportés à la CPS susceptibles d'affecter l'acceptation du service par les professionnels leur seront notifiés par courriel dans le respect des ententes contractuelles en place ou sur le site Web du PSC/R.
- La ***publication du statut d'un certificat*** par le PSC/R constitue un avis aux tiers utilisateurs. Dans cette optique, un certificat est considéré comme révoqué par les tiers utilisateurs dès la publication de cette information.
- Les conditions générales et particulières d'utilisation des produits de Notarius sont publiées sur son site Web, tout comme les ANS. Elles sont donc disponibles 24h/24 et 7j/7.

2.3 Conservation et accès aux versions antérieures

Notarius conserve l'ensemble des versions antérieures de ses CP et de la présente CPS. Ces versions peuvent être mises à disposition sur demande auprès de l'Autorité de certification, conformément aux exigences de transparence du Mozilla Root Store Policy, des normes ETSI et des critères WebTrust.

2.4 Informations non publiées

Notarius ne publie jamais :

- de données personnelles d'abonnés ;
- d'informations d'identification recueillies lors des processus d'enregistrement ou de validation ;
- de renseignements de nature confidentielle tels que définis par les lois applicables.

Toute transmission de données hors du répertoire public doit respecter la politique de

confidentialité et les exigences légales en vigueur.

2.5 Point de contact et déclaration d'incident

Notarius maintient un mécanisme public permettant à toute personne (abonné, partie de confiance, chercheur en sécurité, tiers) de déclarer :

- un incident de sécurité ;
- un problème affectant un certificat ;
- un comportement anormal ou non conforme ;
- une vulnérabilité potentielle.

Ce mécanisme est accessible via :

- Formulaire de signalement : https://www.notarius.com/fr/soumettre-vulnerabilite
- Courriel PKI dédié : officiers@notarius.com

Toutes les déclarations reçues sont traitées selon la procédure interne de gestion des incidents applicable à l'Autorité de certification.

3 Identification et authentification

Cette section décrit les exigences et pratiques de Notarius en matière d'identification des abonnés, de vérification des organisations, de validation des attributs contenus dans les certificats et de contrôle des informations critiques, incluant notamment l'adresse de courrier électronique lorsque celle-ci apparaît dans le certificat (RFC 822Name).

Les processus décrits dans cette section sont appliqués par les personnes autorisées du PSC/R et par les agents accrédités (ALE, AVA, AVI), sous la supervision de l'Autorité de certification.

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.
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.

Certaines composantes du DN utilisées par Notarius ont des longueurs autorisées (limites) prédéfinies de caractères :

- CN (Common Name) : 64
- O (Champs certifié par le CRM) : 64
- OU (Nom du produit) : 64
- C : 2

3.1.2 Noms explicites

Les noms choisis pour désigner les détenteurs de certificats sont explicites.
Le common name (CN) d'une personne physique est construit à partir des noms et prénoms du détenteur tel que validés lors de sa vérification d'identité ou provenant du tableau de son Ordre professionnel le cas échéant.
Pour les certificats délivrés à des organisations, départements, groupes, applications ou dispositifs, l'identité de l'entité est validée préalablement.

Le DN comprend notamment:

- Le nom du détenteur (ou celui d'un groupe, d'un rôle, d'un dispositif ou d'une application auquel le détenteur veut affecter les clés et les certificats);
- Pour les détenteurs membres d'un RPR, le matricule professionnel ;
- Pour les autres détenteurs, un code d'identification administratif ;
- L'identification ou l'acronyme du groupe auquel le détenteur appartient.

3.1.2.1 Détails des produits CertifiO (AATL et Non AATL)

Produit	**uid (*unique ID*)**	**cn (*common name*)**	**ou= (*champs Certifié par du CRM*)**	**o= (*nom du produit*)**	**c=CA**
CertifiO pour évaluation	*Identifiant composé de caractères aléatoires*	Test - *Prénom du contact Nom du contact -- Nom du compte* *(attention, **si** produit d'évaluation, alors sera nécessairement Notarius Évaluation)*	*Nom dans le DN du compte* **ou** *Nom du compte*	CertifiO Test CertifiO Test - AATL	c=CA
CertifiO pour professionnels	*No. de membre*	*Prénom du contact Nom du contact -- Titre professionnel - Nom court du compte* **ou** *Nom dans le DN du compte* **ou** *Nom du compte*		CertifiO Pro CertifiO Pro - AATL CertifiO Pro - Cloud	c=CA
CertifiO pour employés	*Courriel professionnel*	*Prénom du contact Nom du contact -- Nom court du compte* ***ou*** *Nom dans le DN du compte* ***ou*** *Nom du compte*		CertifiO - Empl. CertifiO - Empl. - AATL CertifiO - Empl. - Cloud	c=CA
CertifiO pour départements	*Identifiant composé de caractères aléatoires*	*Nom du département -- Nom court du compte* **ou** *Nom dans le DN du compte* **ou** *Nom du compte*		CertifiO - Dept. CertifiO - Dept. - AATL CertifiO - Dept. - Code	c=CA
CertifiO pour organisations	*Identifiant composé de lettres et de chiffres*	*Nom court du compte* ***ou*** *Nom dans le DN du compte* ***ou*** *Nom du compte* ***ou*** *Nom spécifié par le client** *(*) Dans les cas du Nom spécifié par le client, le double tiret n'est pas acceptable si ce dernier souhaite voir affiché au complet ledit Nom spécifié*		CertifiO - Org CertifiO – Org - AATL CertifiO - Org - Code	C=CA

3.1.2.2 Exemples

Produit	Exemple	Résultat pour le DN
CertifiO pour évaluation - Notarius Tests internes	Signature de test pour le SAC	uid=12345+cn=Test - John Do -- Solutions Notarius, ou=Solutions Notarius, o=CertifiO Test, c=CA
CertifiO pour évaluation - Général	Signature de test pour un client non identifié dans le CRM Produit d'évaluation	uid=12345+cn=Test - Monsieur Untel -- Notarius Évaluation, ou=Notarius Évaluation, o=CertifiO Test, c=CA
CertifiO pour professionnels	Signature pour un ingénieur	uid=654321+cn=John Do -- ingénieur - OIQ, ou=OIQ - Ordre des ingénieurs du Québec, o=CertifiO Pro, c=CA
CertifiO pour employés	Signature pour un employé	uid=john.do@notarius.com+cn=John Do -- Solutions Notarius, ou=Solutions Notarius, o=CertifiO - Empl. - AATL, c=CA
CertifiO pour départements	Signature pour le Marketing	uid=D2A585ED+cn=Marketing -- Solutions Notarius,ou=Solutions Notarius,o=CertifiO - Dept. - AATL,c=CA
CertifiO pour organisations	Signature pour courriel du SAC sur jeton	Service à la clientèle -- Solutions Notarius, ou=Solutions Notarius, CertifiO - Org - AATL, c=CA

3.1.3 Anonymisation ou utilisation de pseudonyme

Les pseudonymes ne sont pas autorisés.

3.1.4 Règles d'interprétation des 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 dépendent du type de certificats émis.

3.1.5 Unicité des noms

Notarius garantit l'unicité du DN pendant toute la durée de vie de l'AC, grâce au numéro de série unique et aux éléments constitutifs du DN.

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

3.1.6 Marques déposées

Le demandeur est responsable de s'assurer que le nom demandé ne viole pas des droits de propriété intellectuelle. Notarius ne procède pas à des recherches d'antériorité.
Le droit d'utiliser un nom qui est une marque de commerce, de service ou autre appartient au titulaire légitime de cette marque ou encore à ses licenciés ou cessionnaire. 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. Notarius ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par les clients et bénéficiaires des marques déposées, des marques enregistrées, des signes distinctifs ou autre, ainsi que des noms de domaine.

3.2 Validation de l'identité

Le PSC/R se réfère à NIST 800-63A pour la fiabilité des pièces d'identité (« *Superior* », « *Strong* » ou « *Fair* »).

En effet, bien que ces pièces n'aient pas toutes la même fiabilité, elles supposent toutes que l'émetteur a effectué une forme de vérification de l'identité du demandeur avant leur délivrance.

Les pièces d'identités de type « *Fair* », « *Strong* » et « *Superior* » doivent toujours être émises par une autorité gouvernementale reconnue :

- « *Strong* » ou « *Superior* »: doit être délivrée dans un contexte de service au citoyen et non à un employé (ie: une carte d'employée de l'état n'est pas permise)
- « *Fair* »: peut être une carte d'employée du gouvernement si et seulement si le PSC/R est confiant que l'entité gouvernementale a fait une vérification d'identité avant de procéder à l'émission. À ce titre, il a été décidé que seuls les gouvernements fédéraux et provinciaux (ou États aux USA), ainsi que les agences et sociétés d'état, se qualifient.

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

Dans le respect des Règles d'affaires pour vérification d'identité et d'affiliation.

Les principes sont les suivants :

- La ***vérification de l'identité (VI)*** doit être réalisée par un AVI autorisé par le PSC/R :
  - À distance par un employé autorisé de Notarius.

- La ***vérification de l'affiliation (VA)*** doit être réalisée par un AVA pour entreprise ou pour professionnels dont les pouvoirs auront été formellement délégués par son ALE. L'ALE aura formellement autorisés et identifié ses AVA auprès de Notarius.
  - La procédure de nomination des AVA doit être suivie.
  - Des formulaires doivent être complétés, signés et retournés au PSC/R.

- Une personne qui effectue la VI d'un client donné ne peut pas agir comme celui qui

vérifie la conformité du processus (RCI) pour ce même client.

Les vérifications servent à établir l'identification et l'existence d'une personne physique, d'une personne morale, d'un dispositif, d'une application ou d'un groupe (d'un département).

Le tableau des Règles d'affaires pour l'ICP de Notarius montre les vérifications exigées en fonction du produit/certificat demandé :

Produit ***Activité***	**CertifiO pour Professionnels**	**CertifiO pour Employés**	**CertifiO pour Organisations**	**CertifiO pour Départements**	**CertifiO Évaluation**
Type de VI	DI ou RC	DI ou RC	Vérification de l'entreprise (pas de VI du demandeur)	Vérification de l'entreprise (pas de VI du demandeur)	Aucun
Type de VA	Ordre	Employeur	Entreprise	Entreprise	Aucun

Légende :

Type de VI

- DI = À distance avec croisement de données
- RC = Répondant de confiance (ex. un employé de Notarius ou un notaire détenant une sn de Notarius)

3.2.1 Validation de l'adresse de courrier électronique et contrôle du domaine

Pour tout certificat contenant une adresse de courrier électronique (RFC 822Name), Notarius procède à une validation directe du contrôle de cette adresse au moyen d'un mécanisme de vérification de type *challenge-response*.

Un message électronique contenant un lien unique ou un code de validation temporaire est envoyé à l'adresse déclarée. Le demandeur doit compléter cette étape afin de démontrer qu'il contrôle la boîte de réception associée.

Aucun certificat contenant une adresse courriel n'est émis tant que cette validation n'a pas été complétée.

Notarius ne délègue pas la validation du contrôle des adresses de courrier électronique ni des noms de domaine.
Les organisations clientes peuvent fournir des renseignements facilitant l'identification, mais la validation technique du contrôle du courriel est réalisée exclusivement par Notarius. L'absence de validation entraîne le rejet automatique de la demande.

Cette validation doit être complétée avant la vérification d'identité.

3.2.2 La vérification initiale de l'identité

Le processus de vérification de l'identité initiale ne débute que lorsque le détenteur a, dans l'ordre :

- Rempli son formulaire d'adhésion en ligne *(cette activité peut être réalisée également par l'acheteur)*
- Accepter les conditions générales d'utilisation du produit
- Procédé au paiement *(cette activité peut être réalisée également par l'acheteur)*
- Fait confirmer/valider son courriel professionnel par le PSC/R
- Défini son mot de passe de compte et 2ème facteur d'authentification
- Planifié sa vérification d'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 pièces justificatives telles des documents officiels valides émanant d'une autorité gouvernementale reconnue. La pièce principale présentée doit inclure les prénoms(s), nom(s), date de naissance, photo et signature du demandeur. La deuxième ou troisième pièce (si requise), qui sert à augmenter le niveau de confiance et non à assurer de l'exactitude, devra mentionner au minimum les prénom(s) et nom(s).

Les informations relatives à l'identité du demandeur et portées dans le certificat doivent correspondre aux informations présentées dans le cadre de la vérification d'identité, à celles du formulaire d'adhésion ou à celles de l'inscription au tableau de l'Ordre professionnel pour les signatures CertifiO pour professionnels.

L'ensemble des pièces d'identités soumises doivent permettre à l'AVI de différencier les individus, incluant les homonymes, peu importe les attributs.

Un tiers doit également pouvoir identifier le détenteur avec un niveau de confiance élevé, même s'il existe des différences mineures entre le nom légal, le nom usuel ou le nom inscrit au tableau de l'Ordre.

La demande initiale de clé et de certificat nécessite toujours une vérification de l'identité du demandeur via vidéoconférence (en direct ou suite à la prise de rendez-vous) avec l'AVI du PSC/R, sauf pour CertifiO Test ou Évaluation.

Lorsque les moyens technologiques le permettront et, dans le respect de ETSI EN 319 411-1, section 6.2.2, la vérification de l'identité des détenteurs pour l'émission d'un second certificat de signature numérique, pourra également être réalisée au moyen de leur premier certificat de signature, délivré conformément au processus de vérification initiale de l'identité ci-avant expliqué. La vérification initiale de l'identité devra avoir été réalisée il y a moins de 24 mois.

Une fois l'identité vérifiée l'affiliation à un RPR sera exigée lorsqu'applicable. Auquel cas,

l'affiliation devra être confirmée par le RPR concerné via son AVA ou via le Processus d'approbation et de révocation automatisé. La confirmation d'emploi pour les signatures pour employés sera également exigée lorsqu'applicable.

Dans le cas d'un ***certificat affecté à un groupe, un dispositif ou une application***, le PSC/R doit dans un premier temps s'assurer de l'existence légale de la personne morale. La V.P finances et administration ou son adjointe procédera à cette recherche sur les différents sites dédiés aussi bien au Canada, au Québec qu'à l'étranger. Une copie de cette vérification d'existence est déposée dans le compte CRM de l'entité. Une fois fait, le PSC/R doit s'assurer de l'affiliation avec la Personne morale concernée.

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

Pour être un répondant autorisé, la personne doit être un employé autorisé (AVI) du PSC/R.
La vérification d'identité nécessite la complétion du formulaire spécifié accompagné de la présentation de pièces justificatives (voir section précédente).
La vérification d'identité se réalise habituellement via vidéoconférence par l'AVI autorisé du PSC/R, en direct s'il est disponible ou via la prise de rendez-vous.

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 environnement 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, la Directrice Conformité et gestion des risques, la Conseillère principale Conformité et l'Officier de Notarius.

3.2.4 Liste des pièces justificatives autorisées

Les pièces justificatives, au nombre d'une (1), deux (2) ou trois (3) selon les cas, doivent être valides et émaner d'une autorité gouvernementale reconnue. Seules les pièces originales en caractères latins sont acceptées

Le site Web de Notarius détaille cette liste.

- La ***pièce principale*** présentée doit inclure, en plus d'une photo et signature, les prénoms(s), nom(s) et date de naissance correspondant à ceux du formulaire Web d'adhésion du futur détenteur. Voici en exemple la liste des pièces principales acceptées pour le Canada :
  - Permis de conduite ou carte d'identité provinciale
  - Passeport
  - Carte Nexus
  - Carte d'assurance maladie (distincte du permis de conduire)
  - Carte de citoyenneté
  - Carte de résident(e) permanent(e)

- La ***pièce secondaire*** doit mentionner raisonnablement (*) les prénom(s) et nom(s). Par exemple :

- Toute pièce principale additionnelle
- Carte d'assurance sociale
- Certificat de naissance gouvernemental
- Carte d'employé émise par une autorité gouvernementale fédérale ou provinciale, incluant les agences gouvernementales et entreprises parapubliques, ainsi que la carte d'identité militaire (exclut les villes et municipalités).
- Permis de possession d'arme ou permis de chasse avec photo
- Carte PIV ou PIV-I
- Carte de statut autochtone

L'AVI du PSC/R se réserve le droit d'effectuer des vérifications additionnelles ou ultérieures avant de délivrer un certificat de signature numérique en demandant par exemple la présentation d'une troisième pièce d'identité.

(*) La pièce secondaire sert à augmenter le niveau de confiance et non à assurer de l'exactitude. Certains écarts avec la demande peuvent donc être acceptés. Le principe étant que l'ensemble des pièces soumises permette de différencier les individus incluant les homonymes, peu importe leurs attributs (ex. courriel, l'Ordre, etc.). Aucune différence qui pourrait laisser croite qu'il s'agit d'une autre personne ne seront tolérées. En ce sens, certaines différences sur les pièces secondaires seront acceptées par l'AVI du PSC/R par exemple des différences entre gouvernements reconnus (un deuxième nom de famille sur la pièce secondaire qui n'est ni présent sur le formulaire d'adhésion ni sur la première pièce); en raison de conventions sociales (ex. un 2ème prénom absent ou avec initiale seulement) ou encore en lien avec une différence mineure avec le tableau de l'Ordre (un h absent par exemple).

Critères de comparaison utilisées par l'AVI du PSC/R :

- Pour les noms de famille
  - Ignorer la ponctuation (point, apostrophe).
  - Le(s) nom(s) de famille figurant sur la pièce d'identité principale doivent être identiques à la demande.
  - Le(s) nom(s) de famille figurant sur la pièce d'identité secondaire doivent être parmi ceux de la demande, OU le(s) nom(s) de famille sur la demande doivent être parmi ceux figurant sur la pièce d'identité secondaire (ex.: "caballero" vs "caballero guerrero")

- Pour les prénoms
  - Ignorer la ponctuation (point, apostrophe)
  - Si la demande ne comporte pas d'initiales, alors les initiales sur les pièces d'identité peuvent être ignorées
  - Si la demande comporte une ou des initiales, elles doivent correspondre aux initiales des prénoms ou initiales correspondants présentent sur l'une des pièces d'identité. Ceci inclut le premier prénom comme initiale.

- Le(s) prénom(s) et nom de famille figurant sur la pièce d'identité principale doivent être identiques à la demande, à l'exception des initiales pour lesquelles les règles ci-haut s'appliquent.

3.2.5 Vérification de l'affiliation

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 (manuellement ou via le processus d'approbation et de révocation automatisé) l'affiliation du demandeur signifie que celui-ci est un membre en règle de son Ordre professionnel ou un employé de ce RPR, et qu'il est autorisé à détenir une signature numérique.
- 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 des produits CertifiO pour employés ou pour professionnels équivaut également à une présomption de confirmation d'affiliation ou de lien d'emploi.

Dans le processus d'approbation et de révocation automatisé, le PSC/R accepte quelques différences des noms et prénoms entre les informations de la demande et les informations du tableau de l'Ordre professionnel, soit :

- Pour les noms de famille
  - Les accents et tirets peuvent différer
  - L'acronyme "St" peut être interchangé avec "Saint", et "Ste" pour "Sainte"
  - Les noms composés peuvent être joints ("Mc Culloch" vs "McCulloch", "Mac Arthur" vs "MacArthur")
  - Des noms de famille additionnels figurant sur la demande ne sont présent que sur la pièce d'identité secondaire (commun pour les noms hispaniques)
  - Une autorisation d'un AVA de l'Ordre ou d'un Officier lorsque des noms de familles additionnels sont présent uniquement sur la demande ou uniquement sur les 2 pièces d'identité (commun pour les noms hispaniques)

- Pour les prénoms
  - Les accents et tirets peuvent différer
  - Les noms composés peuvent être joints ("Van Deth" vs "VanDeth", "Marie-Anne" vs "Marieanne")
  - Les articles de liaison peuvent être ignorés ("Maria de Fatima" vs "Maria Fatima", commun pour les noms hispaniques)
  - Des prénoms additionnels figurant sur la demande ne sont présent que sur la pièce d'identité secondaire (commun pour les noms hispaniques)
  - Une autorisation d'un AVA de l'Ordre ou d'un Officier lorsque des prénoms additionnels sont présent uniquement sur la demande ou uniquement sur les 2 pièces d'identité (commun pour les noms hispaniques)

3.2.6 Critères d'interopérabilité

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

L'ICP de Notarius est reconnue par le Capi de Microsoft.

3.2.7 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 et de l'usage exclusif des données d'activation.

Une fois la VI et la confirmation du lien d'emploi complétées avec succès par courriel, la demande est finalisée par l'employé autorisé du PSC/R. .
Un courriel est automatiquement transmis au demandeur l'informant de l'approbation de sa demande d'adhésion ou bien un bouton sera disponible dans son portail-client pour continuer sa demande.
Un code de référence lui est alors transmis et il est également invité à activer son certificat.
Les données d'activation permettant de générer le certificat du détenteur lui sont finalement remises après qu'il s'est authentifié au portail du PSC/R au moyen de son courriel et mot de passe de compte, connues de lui seul, et recueillies lors de son inscription.

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

Le détenteur est avisé avant l'expiration, à l'avance, par courriel (plusieurs envois sont faits T-30, T-15, T-5, 0 jour) de l'imminence de l'expiration de ses clés et ses certificats.
Trente (30) jours avant la date d'expiration, si le détenteur utilise sa signature numérique en ligne, le renouvellement se fera automatiquement via Entrust.
Dans la plupart des cas, cette mise à jour du certificat est réalisée automatiquement.
Le détenteur recevra alors un courriel de confirmation en cas de succès.
En cas d'échec du processus de renouvellement automatique, le détenteur sera avisé par courriel que ladite mise à jour n'a pas fonctionné et que la signature expirera et le certificat révoqué.

- Si l'abonnement du détenteur est encore actif : le détenteur pourra demander la récupération de son certificat en s'authentifiant sur le portail client "Mon compte Notarius". Dans le cas contraire (abonnement inactif ou expiré), le détenteur n'aura d'autre choix que de se réabonner et de refaire le processus au complet, soit VI selon les cas et autorisation du RPR.

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

Chez le PSC/R on parle à l'interne de « réabonnement ».
Lorsque le détenteur demande la réémission de ses clés et ses certificats dans un délai de douze (12) douze mois suivant leur révocation, leur expiration ou leur annulation, il devra s'authentifier avec succès au portail client "Mon compte Notarius".
À défaut, le détenteur devra à nouveau faire vérifier son identité selon la procédure prévue à

la section 3.2.1.
Les réémissions ne sont pas applicables pour CertifiO Organisation. Une nouvelle émission est privilégiée.

3.2.10 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 son portail client « Mon compte Notarius » à l'aide (de son mot de passe & 2ème facteur d'authentification si requis ou autre certificat de signature numérique valide lorsque la technologie le permet) afin de procéder lui-même aux changements souhaités *(*les champs modifiables sont : le titre, le courriel professionnel, le courriel secondaire, les coordonnées téléphoniques, le numéro de téléphone de 2ème facteur d'authentification, le moyen de 2ème facteur d'authentification, 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 service à la clientèle du PSC/R pour qu'une demande de modification soit ouverte en son nom via un billet (appel de service).
La mise à jour de renseignements comme le prénom ou le nom nécessitera la vérification préalable 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 demandés dans SMA.

Pour les détenteurs de certificats pour organisation ou départemental, une demande formelle auprès du responsable identifié du PSC/R (au département des ventes ou encore de la gestion des produits) sera requise pour que l'Officier du PSC/R procède manuellement après les vérifications d'usage au dossier client, aux changements demandés et pose les actions requises avec le chef d'équipe TI lorsque de besoin.

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 (l'Acheteur) peut initier le processus d'abonnement et demander des clés et des certificats pour elle-même, ou pour un Détenteur autorisé.
Une personne morale peut demander des clés et des certificats pour ses employés ou pour un de ses dispositifs ou de ses applications. Dans ce dernier cas, elle devra désigner une personne physique pour agir comme responsable.

4.1.2 Procédure d'adhésion

L'Acheteur qui souhaite obtenir des clés et des certificats pour lui-même ou pour un Détenteur autorisé doit:

- Faire une demande auprès du PSC/R via les formulaires prévus à cet effet en :
  - Entrant les informations du détenteur de la signature.
  - Entrant les informations de l'acheteur (si différentes).
- Vérifier les renseignements saisis et choisir un mode de paiement
- Accepter les conditions générales d'utilisation du produit;
- Acquitter les frais afférents;
- Le détenteur doit valider/confirmer son courriel professionnel
- Le détenteur doit définir son mot de passe de compte et 2ème facteur d'authentification dans le portail libre-service
- Faire vérifier l'identité du détenteur 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 processus d'adhésion pour CertifiO Organisation diffère légèrement en ce sens que la signature d'une entente contractuelle formelle préalable est requise pour initier le processus d'adhésion (tous les contrats sont répertoriés par le PSC/R). Le client devra remplir le formulaire d'ouverture de compte transmis par l'équipe des ventes ou les services administratifs du PSC/R. Ce processus implique, en plus du client, l'équipe des ventes du PSC/R, l'Officier ICP et les équipes de produit et TI.

4.2 Approbation ou refus de la demande

À la réception d'une demande, une fois la vérification de l'identité réalisée, des validations manuelles ou automatisées sont faites (vérification et cohérence des attestations ou documents fournis) par le PSC/R ou l'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.
L'Autorité de certification conserve en tout temps la responsabilité finale de toutes les décisions d'émission, même lorsque certaines vérifications, telles que les validations

d'affiliation ou de lien d'emploi, sont effectuées par un RPR, un AVA ou un représentant autorisé.

4.2.1.1 Acceptation ou refus d'une demande de signature numérique corporative ou départementale

Les demandes d'adhésion d'une signature corporative ou départementale sont confirmées ou refusées par l'AVA de l'ALE, sur réception d'un courriel transmis automatiquement par le PSC/R.
La confirmation du bien-fondé ou du 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 l'entité, du lien d'appartenance ou d'emploi via la plateforme de gestion des signatures numériques de Notarius à accès restreint.

4.2.1.2 Acceptation ou refus d'une demande de signature pour organisation

Le processus d'adhésion débute toujours par la négociation/signature de l'entente contractuelle. Au moment de la signature du Contrat, le formulaire d'ouverture de compte identifiant les contacts autorisés de l'organisation signé par le responsable du compte sera transmis à la comptabilité pour validation des informations de l'entreprise (validation d'entité).
Une fois tous les documents reçus et les validations effectuées, alors seulement l'Officier du PSC/R pourra poursuivre les activités de création des certificats.

4.2.1.3 Acceptation ou refus des autres types de demande de signature

Les demandes d'adhésion sont traitées soit manuellement par l'AVA du RPR via la plateforme de gestion des signatures numériques de Notarius soit automatiquement via le processus d'approbation et de révocation automatisée

4.2.1.4 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 à l'acheteur lorsque celui-ci a payé par carte de crédit.

Il est à noter que, dans de très rares cas d'indisponibilité avérée des AVA d'un RPR, le responsable du RPR pourra communiquer avec le PSC/R pour lui demander de procéder en son nom. Un courriel formel, une liste détaillée et les cas de refus seront requis. Un billet sera également ouvert dans le CRM avec les preuves permettant ainsi à l'Officier du PSC/R de procéder au nom du RPR.

4.2.1.5 Types de décisions pouvant être prises via le processus d'approbation et de révocation automatisé

Deux (2) types de décisions peuvent être prises :

1. **Approuver** : approbation de la demande sélectionnée, telle quelle.
2. **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 à l'acheteur lorsque celui-ci a payé par carte de crédit.
   - Pour les cas de non-concordance des informations nominatives entre la demande et les informations contenues au tableau de l'Ordre professionnel, l'acheteur sera invité à communiquer avec le support à la clientèle du PSC/R ou avec l'AVA de son RPR.

4.2.2 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.

4.2.3 Approbation d'un certificat

Plusieurs cas peuvent se présenter selon le type de certificat approuvé.
Par principe le détenteur est notifié par courriel de l'approbation de sa demande.
Son jeton AATL lui est transmis par courrier recommandé, au besoin.
Il est invité à activer sa signature numérique à la suite de la génération de son certificat.
Il est alors présumé avoir accepté les clés et les certificats dès leur activation.

Dans les cas d'approbation des certificats pour organisations, les étapes sont décrites dans des processus internes dédiés.

4.3 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.
Lorsque le certificat contient une adresse de courrier électronique (RFC 822Name), le contrôle de cette adresse est revérifié avant tout renouvellement, conformément aux exigences applicables.
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.

Pour CertifiO Organisation, l'Officier du PSC/R gère les dates de fin attendue des certificats afin de procéder manuellement à la mise à jour du certificat système lorsque requis.

4.3.1 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;
- L'Officier du PSC/R

4.3.2 Procédure de demande de renouvellement d'un certificat

En fonction des *certificate policies*, la période de validité des certificats délivrés par l'AC peuvent être de 24 mois, de 36 mois ou plus à partir de leur date d'émission. Par exemple, le certificat pour organisation peut être valide 10 ans et sa clé privée 3 ans.
Le processus de renouvellement débute à un certain pourcentage de durée de vie du certificat (informations également disponibles dans les *certificate policies*).
Le processus est initié automatiquement par le détenteur lors de l'utilisation de sa clé privée dans un dispositif ou manuellement par l'Officier.

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

Excepté pour les certificats d'organisations traités manuellement par l'Officier du PSC/R, le processus de renouvellement des autres types de certificats est initié automatiquement par le détenteur lui-même 30 jours avant la date d'expiration de sa clé privée dans les cas où il 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.

4.3.4 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 le dossier du contact (dans le CRM du PSC/R).

Le détenteur est notifié dès la génération de son certificat par le dispositif comme suit :

- *30 jours* avant la date d'expiration de sa clé privée, le détenteur est avisé que sa signature numérique demande son attention;
- *15 jours* avant la date d'expiration de sa clé privée, un 2e avis lui est transmis;
- *5 jours* avant la date d'expiration, la notification indique que sa signature numérique ne sera plus fonctionnelle dans 5 jours;
- *0 jour* un avis indiquera finalement au détenteur que sa signature numérique n'est plus fonctionnelle.

4.4 Récupération d'un certificat

La récupération consiste en l'émission de nouvelles clés (et même d'un nouveau Certificate ID pour les CEV) et de nouveaux certificats alors que la clé privée existante est encore valide, mais non fonctionnelle par exemple en raison de la perte du mot de passe liée à la clé privée ou encore 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

4.4.1 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).

4.4.2 Procédure de récupération

Différents types de procédures de récupération peuvent se présenter.

- En ligne;
- En personne.

4.4.3 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.

4.4.3.1 Récupération en ligne

La récupération en ligne est initiée par le détenteur après authentification forte sur le portail du PSC/R. Une fois authentifié, il reçoit les informations nécessaires pour procéder à l'émission d'un nouveau couple de clés et certificats lorsque la clé privée existante est encore valide mais non accessible. Le processus respecte les exigences de sécurité applicables et permet de confirmer que la clé privée n'est pas compromise.

4.4.3.2 Récupération en personne

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

4.5 Demande de modification d'un certificat

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

Les modifications du certificat ne sont pas applicables pour CertifiO Organisation. Une nouvelle émission est privilégiée.

4.5.1 Personnes autorisées

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

4.5.2 Circonstances pouvant entraîner une modification

Une modification peut avoir lieu pour corriger une information contenue au certificat, par exemple une erreur d'orthographe dans le nom ou le prénom ou encore une erreur dans le numéro du membre ou une erreur de choix de produit.

4.5.3 Traitement d'une demande de modification

Le détenteur peut procéder lui-même à la modification de certains renseignements non critiques contenus dans son certificat. Il doit alors s'authentifier à l'aide de ses questions secrètes au portail du PSC/R et effectuer les changements lui-même.
Autrement, une demande de modification écrite du détenteur doit être acheminée au PSC/R afin que l'Officier ICP puisse procéder en son nom.

4.5.4 Avis de modification

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

4.6 Révocation d'un certificat

4.6.1 Causes possibles d'une révocation

4.6.1.1 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 détenteur figurant dans le certificat,
- Les informations du détenteur 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 de son certificat
- Le détenteur, 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 ou de son support),
- Le certificat de signature de l'AC est révoqué (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante),
- Le détenteur n'accepte pas la mise à jour des conditions d'utilisation applicables au produit auquel il s'est abonné,
- 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 l'ALE avant la fin de validité des certificats.

Lorsqu'une des circonstances ci-dessus identifiées 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.
Lorsqu'une suspicion d'émission incorrecte (mis-issuance) ou de non-conformité est portée à la connaissance du PSC/R, une analyse interne est initiée dans un délai maximal de vingt-quatre (24) heures. Si la situation le justifie, l'AC ou le PSC/R procède à la révocation immédiate du certificat concerné.
L'AC ou le PSC/R peut, à sa discrétion, révoquer un certificat lorsqu'un détenteur ne

respecte pas les obligations énoncées dans la CP, incluant les conditions générales ou particulières d'utilisation des produits de Notarius par exemple le non-paiement lors du renouvellement prévu de son abonnement. Le certificat sera alors révoqué par l'Officier ICP au motif que l'abonnement est expiré.
Une fois qu'un certificat est révoqué, il ne peut être rétabli.

4.6.1.2 Certificats d'une composante de l'ICP

Plusieurs circonstances peuvent être à l'origine de la révocation d'un certificat d'une composante de l'ICP Notarius (incluant un certificat d'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 Notarius 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.

La réalisation de l'une de ces circonstances doit être portée à la connaissance de l'AC ou du PSC/R qui posera immédiatement les actions requises.

Ces scénarios sont évalués et traités notamment dans le plan de continuité des activités (PCA) de Notarius volet intégrité, car ils nécessitent des plans d'action différents selon les circonstances.

4.6.2 Origine d'une demande de révocation

4.6.2.1 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, il doit formuler sa demande de révocation sans délai auprès du PSC/R, soit auprès de son service à la clientèle au *(514) 281-6533* ou de l'équipe de conformité à *officiers@notarius.com*.

4.6.2.2 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.

4.6.3 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 manuellement ou via le processus d'approbation et de révocation automatisé dédié
- L'Officier du PSC/R

4.6.4 Traitement d'une demande de révocation

4.6.4.1 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 des certificats d'organisations sont traitées manuellement après confirmation de leur provenance, par l'Officier du PSC/R.

Les demandes de révocation sont traitées dès réception dans un délai maximal de 24h suivant leur réception.

Elles couvrent la réception de la demande de révocation authentifiée jusqu'à la mise à disposition de l'information de révocation auprès des utilisateurs.

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. Il en est de même pour les réponses OCSP.

Une nouvelle LCR peut être publiée avant la prochaine émission planifiée de LCR.

Dès que le ***détenteur*** a connaissance que l'une des causes possibles de révocation de son ressort est effective, il doit procéder comme suit à sa demande de révocation, et ce, sans délai, soit :

- Lui-même via le site web de Notarius – espace Mon compte;
- En communiquant avec le service à la clientèle du PSC/R pour que celui-ci ouvre une demande de service en son nom.
  Une confirmation écrite est alors requise et jointe à l'appel de service.

Un ***RPR*** peut procéder à la révocation des certificats (SN Pro) activés sous son contrôle via le portail du Libre-Service. Par exemple lors de la révocation au tableau d'un membre de l'Ordre professionnel du RPR.

Le RPR devra toutefois faire une demande écrite expresse au PSC/R pour que son Officier procède manuellement à la révocation pour les cas où la signature numérique du membre n'aurait pas encore été activée.

L'***ALE*** peut demander la révocation des signatures corporatives portées à son compte corporatif au PSC/R via un courriel. Le plus souvent ces demandes surviennent suite à la fin d'emploi du détenteur.

L'***Officier ICP*** peut procéder à la révocation des certificats via le portail du PSC/R suite à la demande expresse et écrite du détenteur, du représentant du RPR, du représentant autorisé de l'ALE ou de l'employeur (dans les cas de signatures corporatives notamment).

L'***Officier ICP*** procède également à la révocation des abonnements expirés minimalement une fois par semaine On parlera plutôt de révocation administrative des certificats.

La cause de la révocation doit toujours être indiquée.
Peu importe qui procède à la révocation, la raison/le motif est toujours conservé par le PSC/R mais non diffusé dans la LCR.

4.6.4.2 Révocation des certificats d'une composante de l'ICP

En cas de fin contractuelle, hiérarchique ou réglementaire entre l'AC et un RPR ou entre l'AC et l'ALE avant la fin de validité des certificats émis au nom ou pour le compte de ce RPR ou cette ALE, tous les certificats devront être révoqués.

En cas de cessation des opérations de l'AC pour quelques raisons que ce soient, Notarius s'engage (à moins d'entente contractuelle indiquant d'autres conditions) à fournir sans retard un préavis informant de la cessation de ses activités et à transférer ses responsabilités aux entités qui lui succéderont ou à celles désignées.

Avant de cesser ses activités, Notarius s'engagera dans la mesure du possible à :

- Donner aux utilisateurs et clients détenant des certificats en cours de validité un préavis de six (6) mois les informant de son intention de cesser ses activités en tant qu'AC
- Donner un préavis de révocation à chacun de ses clients
- Révoquer tous les certificats non révoqués ou non expirés à la fin du préavis de six (6) mois, sans autre avis
- Prendre toutes les mesures appropriées pour conserver ses archives
- Se réserver le droit de prendre les dispositions de succession nécessaire à la réémission des certificats par une AC successeur disposant de toutes les autorisations nécessaires pour agir ainsi et qui s'engage à se conformer à toutes les règles essentielles dans la mesure où ses opérations ont au moins aussi sécurisées que les siennes.

4.6.5 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 (statut added dans SMA), aucune notification ne sera transmise au détenteur. Une trace sera toutefois laissée dans son dossier de contact (CRM).
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. La révocation d'un certificat d'une composante de l'ICP doit être effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation d'un certificat de signature de l'AC Serveurs (signature de certificats, de LCR et/ou de réponses OCSP) est

effectuée immédiatement, en particulier dans le cas de la compromission de la clé.
Les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'ICP Notarius sont décrites dans PCA – intégrité.

4.7 Suspension d'un certificat

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

4.8 Fonctions d'information sur l'état des certificats

L'AC fournit à tous les tiers utilisateurs de certificat les informations leur permettant de vérifier et de valider le statut du certificat incluant toute la chaîne de confiance.
Les informations sur l'état de révocation comprennent des informations sur l'état des certificats au moins jusqu'à l'expiration du certificat.

Cette information sur l'état des certificats est disponible 24 heures sur 24 et 7 jours sur 7, et sans restriction géographique.

Ces informations fournies par les LCR ou l'OCSP sont cohérentes dans le temps, et tiennent compte des différents délais de mise à jour des informations d'état pour ces deux méthodes.
Les réponses OCSP sont signées par une composante autorisée de l'ICP et comportent un indicateur de fraîcheur conforme aux délais exigés par les standards internationaux applicables, incluant les exigences de Mozilla. Ces réponses sont produites en temps réel et reflètent l'état actuel du certificat.
Quelques écarts mineurs de temps peuvent toutefois être observés entre les deux méthodes puisque la LCR est publiée directement sur Internet alors que l'OCSP demande un traitement additionnel avant sa publication. La date de révocation inscrite du certificat entre les deux méthodes sera toujours la même cependant.

4.9 Séquestre des clés et entiercement

Le séquestre des clés privées est interdit, de même que les certificats cachets.

Un contrat d'entiercement (C) a été signé par l'AC advenant la cessation de ses activités.

5 Mesures de sécurité physique et opérationnelle

Le PSC/R de Notarius s'engage à mettre en œuvre et maintenir le niveau de sécurité physique exigé pour les locaux d'exploitation des composantes de l'ICP.
Le PSC/R utilise la méthodologie d'analyse de risque pour identifier les menaces et les opportunités, en faire l'évaluation et appliquer, le cas échéant, les mesures ou les contrôles nécessaires.
Le PSC/R est accrédité à la norme ISO 27001 et est certifié eIDAS.

5.1 Mesures de sécurité physique

Le PSC/R possède notamment et maintien à jour une politique de gestion des TIC, une politique globale de sécurité de l'information et une directive pour ses employés.
Ces documents couvrent notamment les contrôles d'accès physique (à ce titre, le PSC/R limite l'accès aux serveurs de production qu'aux personnes identifiées et ayant besoin d'y accéder pour l'accomplissement de leurs fonctions), la protection en cas de catastrophe naturelle, les pannes de services, la protection contre le feu, le vol et les inondations.
Les contrôles sont 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.
Pour les contrôles et les mesures de surveillance des procédures dédiées sont appliquées.
Pour la gestion des accès, consulter la politique de gestion des TIC, (les demandes d'accès sont gérées dans l'application Podio du PSC/R).
Pour tout ce qui touche aux processus de reprise après sinistre, consulter le dossier de Continuité de l'activité du PSC/R.

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 sont dans des édifices géographiquement situés à plusieurs kilomètres l'un de l'autre. Pour des raisons de sécurité, l'identification de ces sites est classée confidentielle.

Les sites détiennent plusieurs certifications qui témoignent du respect des règlements et normes en vigueur ainsi que des 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.

Ces mesures permettent également de respecter les engagements pris dans la CP, dans les engagements contractuels avec les RPR, les ALE ou encore dans les Accords sur les niveaux des services, en matière de disponibilité des services.

Les nouveaux fournisseurs de colocation sont sélectionnés à la suite des résultats d'un processus de sélection rigoureux incluant des visites sur site.

5.1.2 Accès physique

Le PSC/R a défini un périmètre de sécurité physique où sont installés les matériels et les logiciels des composantes critiques de l'ICP assurant les opérations de génération des certificats et de gestion des révocations.
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 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 opérés dans un espace physiquement isolé des autres opérations. Seules les personnes autorisées à accéder aux clés de l'AC Racine peuvent accéder à cet espace.
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.
Les sites où sont entreposés les systèmes informatiques de l'ICP sont dans des édifices situés géographiquement à plus de cinq kilomètres l'un de l'autre. Ces édifices respectent les normes de construction normalement applicables.
Pour accéder aux locaux, des zones de sécurité et de contrôle d'accès doivent être franchies afin de prévenir ou de détecter les accès non autorisés aux systèmes, les dommages et les interférences.
De plus, le PSC/R s'est assuré que ces sites répondent à de hautes exigences de sécurité.
Un rapport annuel des accès aux sites de colocation est transmis sur demande au PSC/R aux fins de contrôle.
Les installations de l'ICP sont donc contrôlées et vérifiées de sorte que seules les personnes autorisées ont accès aux systèmes et aux données.

Voici quelques exemples déjà en place sur au moins un des sites de colocation du PSC/R :

- Accès sécurisé : postes de garde permanents, identification biométrique et reconnaissance faciale
- Vidéosurveillance en circuit fermé 24 h/24, 7 j/7
- Certification de conformité PCI DSS

Sur le site du Laboratoire, si des personnes non habilitées doivent pénétrer dans nos installations, elles font l'objet d'une prise en charge par une personne habilitée qui en assure la surveillance. Ces personnes doivent en permanence être accompagnées par du personnel habilité. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion. Des audits mensuels d'accès au site ont lieu pour vérifier les accès à ce site.

5.1.3 Alimentation électrique et climatisation

Des systèmes de génération et de protection des installations électriques sont mis en œuvre par le PSC/R pour assurer la disponibilité des systèmes informatiques du site d'exploitation de l'ICP.
Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements. Elles permettent également de respecter les exigences de la présente CPS, ainsi que les engagements pris en matière de disponibilité de ses fonctions.
Les installations électriques et de climatisation sont suffisantes pour assurer le bon fonctionnement des opérations de l'ICP.
Les sites de production et de relève sont équipés d'un système électrique principal et d'un système de secours afin d'assurer un accès continuel 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.
Une redondance pour le traitement de l'information est en place pour assurer une disponibilité des principaux systèmes critiques.

5.1.4 Vulnérabilité aux dégâts d'eau

Les sites ont été construits ou équipés de façon à assurer la protection contre les expositions à l'eau.
Les moyens de prévention contre les dégâts des eaux pris par nos fournisseurs de colocation permettent de respecter les exigences de la présente CPS.

5.1.5 Prévention et protection contre les incendies

Les sites sont construits ou équipés afin d'assurer la protection contre les incendies.
Ces mesures rencontrent les normes et lois applicables.
La fonctionnalité des extincteurs et gicleurs est revue à intervalles planifiés. Des rapports sont produits annuellement pour confirmer le bon état de fonctionnement.

5.1.6 Conservation et protection des supports

Les supports contenants les données critiques ou toutes autres informations sensibles sont protégés contre tout dommage, détérioration, vol, accès non autorisés et obsolescence.
Ces médias sont manipulés de façon sécuritaire, en fonction de l'information qu'ils renferment.
Dans le cadre de l'analyse de risque, les supports ainsi que les différentes informations intervenant dans les activités liées à l'ICP ont été identifiées et leurs besoins de sécurité définis en termes de disponibilité, de confidentialité et d'intégrité des données, notamment celles conservées dans les journaux, les archives et les logiciels utilisés par l'AC.
Le détail se retrouve dans la Politique de conservation.
Les procédures de gestion des supports protègent contre l'obsolescence et la détérioration des supports pendant la période de conservation des documents.
Des contrôles ont été mis en place au sein du PSC/R pour diminuer les risques liés aux médias. Une politique globale de sécurité, une directive pour les employés incluant des mesures disciplinaires le cas échéant et des communications de sensibilisation sont en place.

5.1.7 Mise hors service des supports

Pour éviter toute perte de confidentialité, des mécanismes de destruction sûre des médias et des supports sont mis en œuvre.
La destruction des médias est effectuée conformément aux procédures internes de destruction sécurisée des données sensibles.
Ces procédures assurent de disposer adéquatement et selon les règles de sécurité en place des supports ayant servi pour le stockage d'informations.
Les supports de stockage (disque dur) de l'AC ne sont pas réutilisés à d'autres fins avant destruction complète des informations liées à l'AC qu'ils sont susceptibles de contenir.
En fin de vie, les supports sont détruits.

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

5.1.9 Relève

Un 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 après un sinistre ou une défaillance du support de stockage.
Les équipements de sauvegarde et les procédures de rétablissement sont régulièrement testés afin de s'assurer de leur bon fonctionnement. Une réplication est également en place pour les serveurs de production.

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 biclé de l'AC.
Les procédures et politiques de sécurité sont communiquées aux employés. Elles sont pour la plupart identifiées dans un espace dédié accessible à tous les employés du PSC /R.
Des procédures sont établies et appliquées pour toutes les opérations du personnel jouant un rôle de confiance pouvant impacter la fourniture du service.
Des mesures et contrôles opérationnels et administratifs sont mis en place par le PSC/R pour assurer la sécurité des opérations de l'ICP.

5.2.1 Rôles de confiance

L'administration de l'ICP 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 pas agir seule et contourner la sécurité du système de l'ICP. Les rôles de confiance sont notamment détaillés dans la matrice des rôles, portion ICP & LS.

Ces rôles sont décrits comme suit :

- ***Officier de la sécurité*** : Responsable de la mise en œuvre des pratiques de sécurité.
- ***Gestionnaire des opérations / Officier ICP*** : 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.
  Le certificat d'Officier permet d'accéder à l'application SMA et LS, de modifier les politiques d'utilisation et d'agir sur tous les certificats y compris ceux de l'AC.
  Actuellement ce rôle est occupé par la Chef, conformité et gestion des risques & par la Vice-présidente finances et administration du PSC/R. Elles seules peuvent ouvrir les fichiers chiffrés des documents de vérification d'identité conservés par le PSC/R.
- ***Administrateur ICP***: Responsable de l'administration et de l'exploitation des systèmes de l'ICP, par exemple effectuer des sauvegardes et la récupération des systèmes. Permet d'accéder aux serveurs de l'ICP: Security Manager (SM) & Security Manager Administration (SMA).
- ***Auditeur Audit Log*** : Individu autorisé à procéder aux audits mensuels des logs des ICP. L'auditeur Audit log a un droit de lecture seulement. Il peut donc voir les logs mais ne peut pas les modifier.
- ***Auditeur LS*** : Individu autorisé à visualiser les demandes d'adhésion et les signatures numériques émises dans le LS.
- ***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.
- ***Responsable de la Confirmation de l'Identité (RCI) dans le LS*** : ce rôle permet de confirmer l'identité des demandes d'adhésion dans le LS.
- ***Vérificateur de l'identité hors LS*** : ce rôle permet de confirmer/vérifier l'identité en personne ou via un moyen technologique reconnu par le PSC/R.
- ***Vérificateur de l'affiliation dans le LS*** : ce rôle permet de confirmer/approuver l'affiliation d'emploi dans le LS.
- ***Facturation*** : ce rôle permet de révoquer un abonnement corporatif lié à un compte.
- ***Détenteur de carte HSM*** : Responsable de détenir une carte HSM nécessaire pour le fonctionnement du module matériel d'entreposage des clés de l'AC.

L'Autorité de certification conserve en tout temps la responsabilité ultime de la sécurité des opérations de l'ICP, même lorsque certaines tâches opérationnelles ou de contrôle sont confiées à du personnel interne détenant un rôle de confiance ou à des prestataires externes dûment encadrés par contrat.
La Matrice rôles de confiance montre la répartition des fonctions entre les ressources du PSC/R.
Les formulaires de confirmation signés témoignent de l'engagement des ressources internes désignées du PSC/R.
La procédure pour la nomination des AVI et des AVA ainsi que les formulaires d'engagement

des AVA Pro témoignent de leur engagement.
Au sein du PSC/R, 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 de l'AC.
Des mécanismes de contrôles d'accès appropriés sont en place.
La vérification des antécédents des personnes détenant des rôles de confiance est revue à intervalles planifiés, aux 4 ans .

5.2.2 Nombre de personnes requises par tâche

Afin de s'assurer qu'une personne agissant seule ne puisse contourner les mesures de sécurité et ainsi porter atteinte à l'intégrité du service offert, le PSC/R s'assure que certaines tâches reliées à la gestion opérationnelle soient réparties entre plusieurs personnes.
Toutefois, plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mise en œuvre. Conséquemment, selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant nécessairement participer, peuvent être différents.
De plus, certaines tâches ou activités critiques doivent suivre la procédure de Demande d'intervention ICP - Opérations critiques et nécessiter l'ouverture de billets Podio ainsi que l'approbation du DG du PSC/R le cas échéant.

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.

Ces contrôles 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. Un porteur de secrets ne peut détenir qu'une seule part.

5.2.5 Analyse de risque

Notarius réalise une analyse de risque afin d'identifier les menaces sur son ICP.

Cette analyse est revue au moins une fois par année ou lors de changements structurels significatifs.

Les résultats de l'analyse ainsi que la déclaration du RSI sont déposés sur le réseau du PSC/R. Cette analyse est classée Confidentielle.

5.3 Mesures de sécurité relatives au personnel

5.3.1 Qualifications, compétences et habilitations requises

Le PSC/R s'assure via une procédure de recrutement documentée qu'il emploie suffisamment de personnes possédant les connaissances, l'expérience et les qualifications nécessaires pour assurer la prestation de service de l'ICP.

La V.P finances et administration, responsable des ressources humaines s'assure que les attributions de ses personnels, amenés à travailler au sein de l'ICP, correspondent à leurs compétences professionnelles. Les descriptions des postes sont détaillées en conséquence.

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.

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 tout détaillé dans la lettre d'embauche de chaque employé du PSC/R.

5.3.2 Vérifications des antécédents

Le PSC/R effectue systématiquement la vérification des antécédents judiciaires de tous ses employés, et ce, dans le respect de la procédure de recrutement.

Des vérifications sont également effectuées à intervalles réguliers (aux quatre ans) pour toutes les personnes occupant un rôle de confiance au sein du PSC/R.

Une personne reconnue coupable d'un crime grave ou de toute autre infraction ne pourra pas occuper un rôle de confiance ou se verra sans délai retirer ce rôle.

Un rappel est fait dans la Directive employés.

5.3.3 Formation initiale

Le personnel du PSC/R pour donner suite à sa journée d'intégration est formé dès son entrée en fonction aux logiciels, matériels et procédures internes de fonctionnement et de sécurité.

Plus spécifiquement, les employés du PSC/R qui occupent des fonctions reliées à la prestation de services de l'ICP ont reçu la formation initiale appropriée pour accomplir leurs tâches spécifiques.

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.
Une mise à niveau à l'interne est donnée individuellement ou en groupe lors d'un changement important dans les procédures, l'évolution des systèmes ou la mise à jour des rôles de confiance. Des formations externes peuvent être également suivies au besoin.

5.3.5 Fréquence et séquence de rotations entre différentes attributions

Sans objet

5.3.6 Mesures disciplinaires

Le PSC/R applique et maintien un processus disciplinaire lorsqu'un employé effectue une action non autorisée. Le processus disciplinaire décrit dans la directive employés peut inclure des mesures allant jusqu'au congédiement et doit prendre en compte la fréquence et la sévérité de l'action non autorisée.
Les mesures disciplinaires sont catégorisées de 1 à 4, soit :

1. Avertissement verbal
2. Avertissement écrit
3. Suspension sans solde
4. Congédiement

Les mesures 2 à 4 conduiront systématiquement à l'ajout d'une note au dossier de l'employé concerné.
Quelques exemples de situation pouvant conduire à l'application des mesures disciplinaires:

- Écrire un mot de passe sur un bout de papier
- Omettre de verrouiller sa session de travail lorsque l'on quitte son bureau
- Diffuser de l'information confidentielle à des personnes non autorisées
- Abus d'utilisation des actifs de Notarius à des fins personnelles
- Conserver et consulter du matériel pornographique sur les actifs de l'entreprise
- Vol d'équipements ou d'informations de l'entreprise

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

Aucun personnel contractuel ne peut exercer un rôle de confiance dans l'ICP.
Les exigences vis-à-vis des prestataires externes sont documentées par contrat écrit. Des ententes de confidentialité sont systématiquement signées.
Les mesures de sécurité du PSC/R s'appliquent à tout personnel contractuel.
Des ententes de confidentialité ainsi que le respect de la politique de sécurité du PSC/R sont prévus. Les fournisseurs externes qui auraient à travailler dans les centres de colocation du PSC/R sont supervisés comme il se doit.

5.3.8 Documentation fournie au personnel

Le PSC/R met à la disposition de son personnel la CP, la CPS, les procédures internes et les manuels d'exploitation, les documents techniques appropriés soutenant la prestation de service de certification, ainsi que tout autre document pertinent afin qu'il puisse accomplir les tâches qui lui sont dévolues.

5.4 Procédure de journalisation (Registre des vérifications)

La journalisation d'évènements consiste à enregistrer des évènements sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.
Les fichiers résultants rendent possibles la traçabilité et l'imputabilité des opérations effectuées. Plusieurs politiques du PSC/R intègrent ces concepts

5.4.1 Type d'évènement enregistré

La journalisation des évènements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.

- Le PSC/R journalise les évènements concernant ses ICP, notamment : Démarrages et arrêts des systèmes informatiques et des applications;
- Tentatives ou opérations touchant les droits et privilèges des rôles de confiance affectés à la prestation des services de l'ICP;
- Changements aux mots de passe des serveurs et des applications sur les serveurs de l'ICP;
- Changements à la politique de création des certificats;
- Tentative d'accès refusée au système de l'ICP;
- Changements des paramètres de sécurité du système;
- Rapports de non-conformité et de compromission de la sécurité de l'ICP

D'autres évènements sont également recueillis. Ils concernent principalement la sécurité de l'information, par exemple :

- Les accès physiques aux zones sensibles;
- Les actions de maintenance et de changements de la configuration des systèmes;
- Les changements apportés au personnel ayant des rôles de confiance;
- Les actions de destruction des supports contenant des informations confidentielles.

En plus de ces exigences, des évènements spécifiques sont également journalisés, par exemple:

- Réception, approbation ou refus d'une demande de certificat (initiale et renouvellement) ;
- Validation d'une demande de certificat ;
- Évènements liés aux clés de signature et aux certificats d'AC (génération via la cérémonie des clés, sauvegarde / récupération, destruction) ;
- Génération des certificats ;
- Publication et mise à jour des informations liées à l'AC.

Les enregistrements des évènements dans un journal contiennent au minimum les informations suivantes :

- Le type d'évènement ;
- L'identifiant de l'exécutant et/ou la référence du système déclenchant l'évènement;
- La date et l'heure de l'évènement ;
- Le résultat de l'évènement.

Les enregistrements pourront également comporter les champs suivants, au besoin :

- Le destinataire de l'opération ;
- Le nom du demandeur de l'opération ou la référence du système effectuant la demande ;
- Le nom des personnes présentes (si l'opération nécessite plusieurs personnes) ;
- La cause de l'évènement ;
- Toute information caractérisant l'évènement.

Les opérations de journalisation sont effectuées en tâche de fond tout au long de la vie de l'ICP.
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 figurent explicitement dans l'un des champs du journal des 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.
Comme les journaux d'événements peuvent contenir des données sensibles et des informations à caractère personnel. Le PSC/R prend des mesures appropriées de protection de la confidentialité des informations personnelles.

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 vérification qui sont sous le contrôle du PSC/R sont conservés minimalement pendant trois (3) ans en conformité avec le calendrier de conservation.

5.4.4 Mesures de protection

Les registres de vérification sont protégés en tout temps afin d'en assurer la fiabilité, la confidentialité, l'intégrité et la disponibilité. Les registres sont accessibles seulement par la console de gestion (SMA) et par une personne autorisée par son rôle et authentifiée par sa signature numérique (par exemple l'auditeur audit log).

Les registres sont constamment chiffrés par le certificat de l'AC et sont ainsi illisibles hors de la console de gestion.
Toute altération à un registre serait détectée rapidement par les vérifications d'intégrité exécutées périodiquement par l'AC.

5.4.5 Système de collecte des journaux d'événement

Le personnel identifié du PSC/R via des droits d'accès spécifiques peut accéder aux journaux des évènements.

5.4.6 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

5.4.7 Évaluation des vulnérabilités

Toutes les composantes de l'AC sont en mesure de détecter toute tentative de violation de l'intégrité de leur fonctionnement.
Les journaux des évènements de type « Alarm » sont analysés mensuellement via la vérification des audits logs de l'ICP. Cette analyse mensuelle permet de vérifier la concordance entre différents évènements et contribuer à identifier toutes les anomalies importantes.
Les enregistrements et actions posées sont conservés à titre de preuves sur le réseau du PSC/R.
Lors du traitement d'informations colligées dans le registre de vérification et touchant la sécurité du système, le PSC/R prend les mesures nécessaires pour diminuer ou éliminer les vulnérabilités.
Les journaux d'évènements liés à la sécurité sont utilisés comme source principale pour détecter, analyser et documenter les vulnérabilités et incidents affectant l'ICP, et pour démontrer la mise en œuvre des mesures correctives.

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.
Il permet également la conservation des pièces liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité. Dans le respect du calendrier de conservation du PSC/R, les informations suivantes sont conservées:

- La CP
- La CPS;
- Les conditions générales d'utilisation;
- Les dossiers complets des demandes de création et de révocation de certificats;
- Les certificats, LCR et réponses OCSP tels qu'émis ou publiés;
- Les journaux d'évènements;
- Les renseignements recueillis pour établir l'identité des détenteurs;
- Les certificats et la clé publique de signature ainsi que les clés et les certificats de

chiffrement;
- Les copies de sauvegarde des données;
- Les dossiers clients.

5.5.2 Périodes de conservation des archives

Dans le respect du calendrier de conservation du PSC/R, les données suivantes sont conservées pour les périodes indiquées :

- 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.

Une copie des données archivées est conservée sur un site secondaire et est protégée par des mesures physiques et cryptographiques. Ce site est conforme aux exigences environnementales, particulièrement quant à la température, l'humidité et la protection contre le magnétisme.

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.
Les moyens et les mesures mis en œuvre pour assurer la protection des archives sont précisés dans la procédure de gestion des sauvegardes et des médias utilisés.

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. 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.

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.

5.5.6 Procédure de récupération et de vérification des archives

Les archives qui se trouvent physiquement chez le PSC/R ou sur son réseau sont accessibles immédiatement aux personnes autorisées.
Les archives conservées à l'extérieur des locaux du PSC/R sont accessibles dans un délai

maximum de 24h.

5.6 Changement des 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 Gestion des TIC.
Ces moyens permettent de minimiser les dommages en cas d'incidents.
Lorsqu'une suspicion d'émission incorrecte (mis-issuance), de compromission ou de non-conformité significative est portée à la connaissance du PSC/R, une analyse interne est initiée dans un délai maximal de vingt-quatre (24) heures afin de déterminer les mesures correctives à appliquer, incluant au besoin la révocation immédiate des certificats impactés.

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 de la CP mais également du respect des engagements notamment pour ce qui touche les fonctions liées à la publication ou la révocation des certificats.
Le plan de continuité des activités est un pilier de l'approche de gestion. Le but du management de la continuité des activités est d'identifier les menaces potentielles pour l'organisation et les impacts sur les opérations que ces menaces pourraient causer, et de fournir un cadre pour construire la résilience organisationnelle avec la capacité d'une réponse efficace.
Ce plan est testé au minimum une fois tous les 2 ans. Il est de la responsabilité du Vice-président Opérations et Stratégie de produits de déclencher ce plan.

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 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.

Émettra une LCR à jour dans un délai maximal de vingt-quatre (24) heures suivant la détection de la compromission. Le PSC/R informe sans délai les exploitants des magasins de certificats et des programmes de confiance concernés (incluant, le cas échéant, les autorités de programmes de navigateurs et de systèmes d'exploitation) des compromissions avérées et des mesures prises, conformément à leurs politiques respectives.

5.7.4 Capacités de continuité d'activité pour donner suite à un sinistre

Le PSC/R dispose d'un plan de continuité d'activité (PCA) permettant de répondre aux exigences de disponibilité des différentes fonctions découlant de la présente CPS, des engagements de l'AC dans cette CPS et des résultats de l'analyse de risque.
Le PCA inclut entre autres le scénario de compromission des clés de l'AC.
Trois documents distincts composent le PCA du PSC/R, soit :

- PCA - politique continuité des affaires
- PCA - cellule crise
- PCA - annexe A Scénarios

5.8 Cessation des activités

La cessation des activités comprend soit un transfert d'activité à une autre entité, soit une cessation totale de l'activité.

- Le ***transfert d'activité*** est défini comme la fin d'activité d'une composante de l'AC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec une nouvelle entité. Dans ce cas de figure et, pour assurer un niveau de confiance constant pendant et après le transfert d'activité, l'AC s'engage à aviser aussitôt ses clients des changements à venir; à mettre en place des procédures dont l'objectif est d'assurer la constance du service notamment.
- La ***cessation d'activité*** est définie comme la fin d'activité d'une composante de l'ICP comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée. Cette cessation peut être totale ou partielle (ex. la cessation d'activité pour un groupe de certificats donnés seulement).

5.8.1 Cessation des activités de l'AC

Dans la mesure du possible, 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.
Dans le cas de la cessation totale des activités de l'AC, l'entité qui a été désignée par la convention d'entiercement assurera la publication des LCR.
En cas de fin de vie de l'AC, la LCR émise par Notarius le sera avec un champs NextUpdate d'une valeur de 99991231235959Z.
Cette dernière LCR ne sera pas émise avant que tous les certificats visés par ladite LCR ne soient expirés ou révoqués.
Advenant les cas où le PSC/R supprimerait de la LCR les certificats révoqués après leur expiration, la LCR n'inclura pas l'extension X.509 "ExpiredCertsOnCRL" telle que définie dans la norme ISO/IEC 9594-8/Recommandation ITU T X.509.
Si le PSC/R décide ou est tenu de mettre fin à un LCR, il émettra et publiera au point de distribution de la LCR correspondant une dernière LCR avec une valeur de champ nextUpdate telle que définie dans la norme ETSI EN 319 411-1 [2], clause 6.3.9. Exigence CSS-6.3.9-06.

Les modalités de transfert des opérations et des responsabilités sont décidées entre l'AC et le PSC/R. La durée minimale du maintien du statut de révocation sera de deux (2) ans tel que précisé dans le contrat d'entiercement.

L'AC s'engagera notamment à :

- Prévenir ses clients par tout moyen de communication approprié;
- Révoquer l'ensemble des certificats émis par l'AC ;
- S'interdire de transmettre à quiconque les clés privées lui ayant permis d'émettre des certificats ou des LCR ;
- Détruire les clés privées et toutes les copies de sauvegarde des clés privées lui ayant permis d'émettre des certificats ou des LCR.

Un scénario particulier a été documenté par le PSC/R advenant la survenance de cette cessation le tout en conformité avec les requis d'eIDAS.

5.8.2 Cessation des activités du PSC/R

Le PSC/R avisera l'AC au moins trois (3) mois à l'avance de son intention de cesser ses activités.
Les modalités de transfert seront discutées et approuvées par l'AC. Elles seront 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.
Cette cessation peut avoir un impact important pour les clients des membres de l'ALE par

exemple. Afin de minimiser les impacts d'une telle situation, le PSC/R devra s'assurer que les clauses du contrat sont respectées; d'une communication adéquate avec les différents intervenants impactés; évaluer la possibilité de transférer les membres de l'ALE a un autre produit.
La procédure suivante s'applique en cas de cessation des activités d'une ALE : Procédure de fin de contrat d'une ALE.

5.8.4 Fin de vie de l'ICP

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 Mesure de sécurité techniques

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 signatures de l'AC est effectuée :

- Dans des circonstances parfaitement contrôlées
  - Les étapes sont documentées dans le Wiki et montées par l'équipe technique
  - Des tests sont réalisés pour valider des étapes de la Cérémonie
- Par des personnes ayant des rôles de confiance préétablis et approuvés par le Comité ISO+ du PSC/R
  - Les rôles de confiance sont détaillés dans le Wiki :
    - Matrice des rôles – portion ICP & LS
    - Matrice des rôles – Portion HSM
  - Des engagements sont signés par chaque personne occupant un rôle
  - Des enquêtes de sécurité sont réalisées par le PSC/R à intervalles planifiés et sauvegardés dans le dossier RH des employés
- Dans le cadre d'une « Cérémonies des Clés » officialisée.

Les clés de signature de l'AC sont donc générées lors d'une cérémonie officielle à l'aide d'une ressource cryptographique matérielle conforme aux exigences du niveau de sécurité considéré (FIPS 140-2).
Les dispositifs cryptographiques utilisés pour la génération de clés de l'AC utilisent un générateur de nombres aléatoires (RNG).
Durant la cérémonie des clés, toutes les opérations sont effectuées dans des circonstances parfaitement contrôlées, par des personnels ayant des rôles de confiance et en suivant des scripts préalablement définis.
Les cérémonies de clés se déroulent dans les locaux du PSC/R sous le contrôle d'au moins deux personnes ayant des rôles de confiance d'Officier de la sécurité ou de Gestionnaire des opérations et en présence d'une personne de l'externe impartiale. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.
La cérémonie fait l'objet d'un procès-verbal (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. Le PV est conservé sur le réseau du PSC/R.

6.1.1.2 Clés des détenteurs générées par l'AC

La génération des clés des détenteurs est effectuée dans un environnement sécurisé. L'AC ne génère jamais la clé privée de signature du détenteur.
Les clés sont générées dans un module cryptographique conforme aux exigences légales, réglementaires ou normatives applicables.
L'application de l'ICP supporte la gestion de deux paires de clés distinctes, l'une servant au chiffrement et l'autre à la signature.
Les paires de clés sont générées à l'aide d'algorithmes cryptographiques conformes aux

spécifications ci-après exprimées et suivant le protocole d'échange PKIX-CMP[3] :

- Les clés de signature sont générées par le détenteur par le biais d'un module cryptographique logiciel ou matériel.
- Les clés de chiffrement sont générées par l'AC.

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 via l'application du PSC/R.
La clé privée de signature est générée et demeure en tout temps sous le contrôle exclusif du détenteur.
Un courriel d'activation de signature numérique incluant un premier code est transmis au détenteur à son adresse de courriel d'adhésion (adresse vérifiée). En activant la commande prévue à cet effet, le détenteur accèdera au portail de gestion du PSC/R, section « Mon compte ».

Le certificat incluant la clé privée de signature sont générés sur le poste du détenteur selon le protocole d'échange PKIX-CMP. Cette clé privée est maintenue sous le seul contrôle du détenteur.
L'AC ne possède que la clé publique du certificat généré.

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, telle que définie à la section 2.
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

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont annuellement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats d'AC ou dans l'émission de certificats détenteurs doivent ou ne doivent pas être modifiés.

- L'algorithme et la taille des clés des AC racine, iCA1 et iCA2 est RSA-4096 bits.
- L'algorithme et la taille des clés des détenteurs de certificat des AC racine, iCA1 et iCA2 est RSA-2048 bits.
- L'algorithme et la taille des clés de l'AC iCA3 (taille des clés serveurs pour un certificat cachet) est de type P-256 (NIST) en ECDSA.
- L'algorithme et la taille des clés des détenteurs de certificat de l'AC iCA3 est de ECC

[3] *Le protocole PKIX-CMP est documenté dans les publications RFC4210 et RFC6712 de l'IETF.*

P-256.
Aucun certificat émis par l'AC n'utilise des longueurs de clés ou algorithmes non conformes (p. ex. RSA < 2048 bits, SHA-1).
Advenant qu'un algorithme utilisé ne répondent plus aux recommandations des organismes nationaux et internationaux compétents, le PSC/R prendra des mesures (pouvant aller jusqu'à la révocation des certificats le cas échéant) pour y remédier dans les délais impartis. Un plan de communication sera également envisagé avec l'équipe Marketing de celui-ci.

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.

Voir la section 7 pour le détail des profils de certificats.

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.
L'utilisation de la clé privée de cachet est limitée au service *CEV Otentik*.
Toute suspicion de compromission d'une clé privée entraîne des actions immédiates conformément à la procédure de gestion des incidents (voir section 5.7).

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 le *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 niveau 3 et EAL *(Evaluation Assurance Level)* 4+ assurent la protection des clés avec un niveau de sécurité jugé acceptable au regard des menaces pesant sur l'intégrité, la disponibilité et la confidentialité. Les QSCD respectent également les normes ETSI EN 419 241-1 et -2 lorsqu'applicables.

Les équipements QSCD sont validés à chaque année par le PSC/R.

Des processus sont mis en place en lien avec le remplacement de ces derniers en cas de changement de statut.
Par exemple, advenant le cas où le jeton transmis au détenteur ne soit plus conforme au standard QSCD référé dans la norme ETSI EN 319 411-2 (SDP-6.5.1-02) pour la génération de certificat qualifié, le PSCR/R fournira au détenteur un nouveau jeton conforme sur lequel il pourra générer une nouvelle clé privé.

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 sont 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 sont jamais archivées ni par l'AC ni par aucune des composantes de l'ICP.

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 6.1.2

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.
L'utilisation de la signature numérique est en effet un droit personnel et en ce sens il est

strictement interdit au détenteur de confier ou encore de divulguer à quiconque les informations permettant de l'utiliser. Une violation de cet énoncé entraînera la révocation immédiate de la signature numérique.
En ce sens, le détenteur doit prendre toutes les mesures nécessaires pour assurer la sécurité et la confidentialité de ses clés privées, notamment en ne divulguant pas le mot de passe qu'il lui a attribué.

Bien qu'une période d'inactivité automatique puisse être configurée pour une application ou un poste de travail, le détenteur doit toujours vérifier que l'accès à ses clés privées est désactivé avant de quitter son poste de travail.
Lorsqu'un détenteur n'utilise plus ses clés et ses certificats, il doit les détruire en supprimant le fichier de manière à ce que les données soient irrécupérables.
Il est à noter qu'une copie des clés privées de chiffrement est conservée par le PSC/R en prévision d'une éventuelle récupération. Ces clés sont chiffrées en tout temps par et à même l'application de l'ICP.

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.
Cette activation peut se faire via le portail client « Mon compte » ou encore directement via EESP (Entrust Entelligence) en s'inscrivant à un ID numérique Entrust.
Cette procédure n'implique en aucun cas une transmission de clé privée au PSC/R.

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. 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.

6.2.13 Évaluation du module cryptographique

Le module cryptographique répond au FIPS 140-2 Level 3.
Il répond notamment aux exigences de sécurité suivantes (liste non exhaustive) :

- Assure la confidentialité et l'intégrité des clés privée de signatures de l'AC durant toute leur durée de vie, incluant une destruction selon des standards de sécurité élevés
- Identifie et authentifie ses utilisateurs
- Création des enregistrements d'audit.

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 les suivantes :

Type	Durée maximale de vie – avant expiration du certificat
AC Racine	20 ans
AC Émettrice	20 ans
Clé de signature pour AC racine, iCA1 et iCA2	3 ans
Clé de signature pour AC iCA3	10 ans
Clé de chiffrement	3 ans
Clé de test	1 an
Service d'horodatage (TSA – Time Stamp Authority)	10 ans
Service OCSP (Online Certificate Status Protocol / Protocole de vérification en ligne)	2 ans

Le PSC/R peut décider de réduire la période de validité maximale de certains certificats, par exemple pour les certificats de test.

6.4 Données d'activation

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, tel que décrit à la section 3.2.2.

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 sont faites dans le cadre d'une cérémonie des clés.
Les données d'activation pour les détenteurs sont accessibles uniquement après que celui-ci s'est 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.
La clé privée du porteur est générée dans un module cryptographique dont la création et la répartition des données d'activation ont été faites lors de la phase d'initialisation et de personnalisation de celui-ci.

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 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 telles qu'exprimées dans les conditions générales d'utilisation des produits de Notarius et dans les ententes contractuelles particulières le cas échéant.
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.

6.4.3 Autres aspects des données d'activation

Sans objet.

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.
Les systèmes et produits sont choisis ou développés en prenant en compte les exigences de sécurité.
Des analyses de risques sont menées lorsque de besoin selon des exigences et procédures documentées.
Un niveau minimal d'assurance de la sécurité offerte sur l'infrastructure informatique des

composantes de l'ICP est défini dans la Politique de gestion des TIC, dans la Politique de Sécurité de Notarius ainsi que dans la Déclaration d'applicabilité du SGSI.
Les exigences de la norme eIDAS sont également documentées et mis en application.
Ces références documentaires, disponibles sur le Wiki du PSC/R 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.

La protection en confidentialité et en intégrité des clés privées d'infrastructure fait l'objet de mesures particulières, découlant de l'évaluation des risques (Classé C) et revues annuellement ou lorsque de besoin.
Des dispositifs de surveillance des systèmes et des procédures d'audit du PKI notamment sont mis en place.

La configuration de l'ICP ainsi que toute modification ou évolution, est documentée et contrôlée par le PSC/R. Toute modification non autorisée est détectée.
La gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'AC. Lors de son premier chargement, on s'assure que le logiciel est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

Le contrôle des développements des systèmes s'effectue comme suit :

- Les logiciels et les matériels sont acquis de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point est défini et documenté;
- Les matériels et logiciels dédiés à l'ICP ne sont pas utilisés pour d'autres activités;
- Les logiciels installés font l'objet d'une recherche de codes malveillants avant leur première utilisation et périodiquement par la suite ;
- Les mises à jour des matériels et logiciels sont installés par des personnels de confiance et formés selon les procédures en vigueur.

L'application de gestion de l'ICP et les réseaux de production sont logiquement séparés des autres composantes du PSC/R.
Cette séparation prévient les accès non autorisés aux applications de production.
Le PSC/R utilise des pares-feux pour protéger les réseaux de production contre les intrusions internes et externes et limite la nature et la source des activités réseau pouvant y accéder.
Le PSC/R exige l'usage d'un mot de passe nécessitant un minimum de caractères et

composer d'une combinaison alphanumérique. Le mot de passe doit être changé sur une base régulière.
L'accès direct aux bases de données ou aux applications supportant les opérations de l'ICP est limité aux personnes identifiées dans la Matrice rôles de confiance pour accomplir leurs fonctions et nécessite des clés et des certificats « rôle de confiance » comportant des droits spécifiques pour y accéder.
L'AC est accessible par des postes informatiques sous contrôle.
Les composantes accessibles de l'ICP sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).
Les autres composantes de l'ICP utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de pare-feu et de routeurs filtrants.
Les ports et services réseaux non utilisés sont coupés.
Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel l'ICP est hébergée refuse tout service, hormis ceux qui lui sont nécessaires, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.
Les équipements du réseau local utilisé par l'AC sont maintenus dans un environnement physiquement sécurisé et leurs configurations sont périodiquement révisées.

6.6 Mesures de contrôle

Les modules servant à la génération des clés ainsi qu'aux opérations cryptographiques sont conformes aux spécifications énoncées à la section 6.2.
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, selon la méthodologie prévue à cet effet.
Le PSC/R utilise des applications ou composantes qui ont été préalablement vérifiées afin de s'assurer qu'elles offrent une garantie acceptable quant à leur qualité et leur rétrocompatibilité et qu'elles respectent les spécifications énoncées à la section 6.2.
Il teste et documente tout changement à l'infrastructure selon les règles internes définies et dans le respect des recommandations du fabricant.
Selon les conclusions de l'analyse de risque, le PSC/R doit vérifier la rétrocompatibilité avec les applications et composantes existantes.

Le PSC/R a des mécanismes de surveillance des systèmes en place.
Lors de l'installation, et de manière périodique, le PSC/R vérifie 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 respectent les objectifs de sécurité informatiques. 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.

La surveillance et la gestion des vulnérabilités est effectuée à échéances planifiées, incluant

des tests de pénétration et de révision de code.

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 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

La présente section décrit les profils techniques des certificats émis par les différentes Autorités de certification (AC) opérées par le PSC/R, ainsi que les profils des réponses OCSP, des jetons d'horodatage (TSA) et des Listes de certificats révoqués (LCR).

Ces profils sont établis conformément :

- aux exigences de la Politique de certification (CP) applicable à chaque AC,
- aux pratiques décrites dans la présente CPS,
- aux normes ETSI EN 319 411-1 et 319 411-2,
- aux normes ETSI EN 319 421 (TSA) et 319 422 (horodatage qualifié le cas échéant),
- aux exigences S/MIME Baseline Requirements (S/MIME BR) lorsque pertinents,
- aux exigences applicables des programmes de confiance reconnus (ex. Adobe AATL, Mozilla).

Les valeurs exactes des DN, OID, extensions X.509 et paramètres cryptographiques sont détaillées dans les tableaux de cette section et varient selon l'AC (par exemple : CCQ, ICA1, ICA2, ICA3).
Ces différences sont intentionnelles et reflètent les usages, les profils CP et les contextes normatifs propres à chaque AC.

7.1 Profils des certificats de l'AC

Les profils décrits ci-dessous couvrent les types de certificats émis par chacune des AC du PSC/R, incluant notamment :

- Certificats d'AC racine
- Certificats d'AC émettrices (intermédiaires)
- Certificats personnels avec identité vérifiée (signature)
- Certificats personnels avec capacités S/MIME
- Certificats organisationnels ou départementaux
- Certificats de cachet électronique (CEV)
- Certificats serveurs
- Certificats de test

Les profils sont structurés afin d'assurer une interprétation uniforme et conforme aux normes X.509, et précisent, pour chaque certificat :

- les attributs du DN,
- les OID des politiques de certification,
- les usages de clés (KeyUsage, EKU),
- les périodes de validité maximales (alignées sur la CP et la section 6 de la CPS),
- les paramètres cryptographiques,
- les extensions critiques et non critiques.

Les profils réels sont fournis dans les tableaux ci-dessous, tels qu'utilisés opérationnellement dans l'ICP.

Les empreintes numériques sont accessibles 24h/24 et 7j/7 directement sur le site Web de Notarius.

- Les informations principales contenues dans les ***certificats de l'AC Racine et des AC émettrices iCA1, iCA2 & iCA3*** sont :

Champ de base	Valeur pour l'AC Racine	Valeur pour les AC émettrices iCA1, iCA2 et iCA3
Empreinte numérique	**Notarius Root Certificate Authority**[1] **(2014-2034):** 1f 3f 14 86 b5 31 88 28 02 e8 7b 62 4d 42 02 95 a0 fc 72 1a **Notarius Root Certificate Authority**[1] **(2021-2036)**: b1 c3 ac 09 77 aa f1 47 e5 82 1a 87 f8 da 32 22 6a 21 06 93	**Notarius Certificate Authority**[2] **(2015-2034) - ICA1:** bb 05 7f 07 4c 92 da db 5e 49 52 43 e2 59 a0 3f e1 6b d6 87 **Notarius Certificate Authority**[2] **(2021-2036) – ICA1**: 77 16 bf f6 1d 97 10 d7 7b 93 f0 7e 33 24 72 6c 5f 33 76 c5 **Notarius Certificate Authority 2**[3] **(2015-2034) - ICA2**: 7f 44 93 cb 96 11 82 3f c3 e1 2d bb 96 e1 b9 ef 93 a6 84 e3 **Notarius Certificate Authority 2**[3] **(2021-2036) – ICA2**: c5 5a f7 c7 c3 1e 93 86 39 7f e8 f6 71 3d 0b 56 bc ef bc 8b **Notarius Certificate Authority 3**[3] **(2019-2034) - ICA3:** c0 99 e4 55 9f f5 17 35 24 23 8e 13 4e ab 7b c3 6d 00 b8 76 **Notarius Certificate Authority 3**[3] **(2021-2036) – ICA3**: ba 6a 66 c3 d4 d4 12 a1 2e e5 d2 27 5b c6 8e f9 b4 8d 71 d8
Issuer DN	cn=Notarius Root Certificate Authority o=Notarius inc c=CA	cn=Notarius Root Certificate Authority o=Notarius inc c=CA
Subject DN	cn=Notarius Root Certificate Authority o=Notarius Inc c=CA	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius inc c=CA
Longueur des clés de l'AC	4096	4096 256 pour ICA3
Key pair algorithm	RSA	RSA ECDSA pour ICA3
Durée maximale avant l'expiration du certificat	20 ans	20 ans

(1) *Notarius Root Certificate Authority = Certificat racine également publié par Microsoft comme racine de confiance dans son magasin de certificats.*
(2) *Notarius Certificate Authority = Certificat d'autorité intermédiaire reconnu d'office par Adobe et Microsoft.*
(3) *Notarius Certificate Authority 2 & 3 = Certificats d'autorités intermédiaires reconnus d'office par Microsoft.*

- Les informations principales contenues dans ***le certificat d'un détenteur pour les AC racine, iCA1 et iCA2*** sont :

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
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.

- Les informations principales contenues dans ***le certificat d'un détenteur*** pour iCA3 sont:

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	ECC P-256
Durée de validité du certificat	6 mois à 10 ans
Extension du certificat	Usage autorisé : AIGCEV User role; Certificate policies; Key usage;SubjectAltName.

- ***Profil du certificat AATL – ICA1***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.2.1.1) Natural person / Personne physique (2.16.124.113550.2.2.2.1) Conforme à Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2) Esi4-qcStatement-1 (0.4.0.1862.1.1) AIA = http://ocsp1.notarius.com/ocsp1-ca1 (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique, Non-Répudiation (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email

- ***Profil du certificat AATL Évaluation – ICA1***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit]

	c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Identity NOT verified / Identité NON vérifiée (2.16.124.113550.2.2.1.0) Natural person / Personne physique (2.16.124.113550.2.2.2.1) Conforme à Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Intended for Adobe test / Pour test Adobe (1.2.840.113583.1.2.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2) AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email

- ***Profil du certificat AATL – CertifiO Cloud***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.2.1.1) Natural person / Personne physique (2.16.124.113550.2.2.2.1) Conforme à Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2) QCP-n-qscd (0.4.0.194112.1.2)

	Esi4-qcStatement-1 (0.4.0.1862.1.1) AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique, Non-Répudiation (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email

- ***Profil AATL HSM – ICA1***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.2.1.1) Legal person / Personne morale (2.16.124.113550.2.2.2.2) Conforme à Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2) AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email

- ***Profil AATL HSM Evaluation – ICA1***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Identity NOT verified / Identité NON vérifiée (2.16.124.113550.2.2.1.0) Legal person / Personne morale (2.16.124.113550.2.2.2.2) Conforme à Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Intended for Adobe test / Pour test Adobe (1.2.840.113583.1.2.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2) AIA = http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = 1 = http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl 2 = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email

- ***Profil Certificat standard – ICA2***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit]

	c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Support logiciel (2.16.124.113550.2.3.3.1) Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.3.1.1) Individual's identity - Identité d'un individu (2.16.124.113550.2.3.2.1) AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl Mail = Email

- ***Profils Standards avec Encryption – ICA2***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Support logiciel (2.16.124.113550.2.3.3.1) Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.3.1.1) Individual's identity - Identité d'un individu (2.16.124.113550.2.3.2.1) AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl Mail = Email

Champ de base	Valeur

Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Support logiciel (2.16.124.113550.2.3.3.1) Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.3.1.1) Individual's identity - Identité d'un individu (2.16.124.113550.2.3.2.1) AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1) Key usage = Chiffrement (2.5.29.15); Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl Mail = Email

- ***Profil Standard d'évaluation – ICA2***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	2048
Durée de validité du certificat	6 mois, 1 an, 2 ans ou 3 ans
Extension du certificat	Certificate policies = Support logiciel (2.16.124.113550.2.3.3.1) Individual's identity / Identité d'un individu (2.16.124.113550.2.3.2.1) Identity NOT verified / Identité NON vérifiée (2.16.124.113550.2.3.1.0) Intended for Adobe test / Pour test Adobe (1.2.840.113583.1.2.2) AIA = http://ocsp1.notarius.com/ocsp1-ca2 (1.3.6.1.5.5.7.1.1) Key usage = Signature numérique (2.5.29.15);

	Extended Key Usage = URL TSA Personnalise (1.2.840.113583.1.1.9.1) CPD = http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl Mail = Email

- ***Profil Certificat standard – ICA3***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	ECC P-256
Durée de validité du certificat	6 mois à 10 ans
Extension du certificat	Certificate policies = Identity verified face-to-face / Identité vérifiée en face-à-face (2.16.124.113550.2.4.1.1) Legal person / Personne moral (2.16.124.113550.2.4.2.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.4.3.2) Intended for server automation / Pour serveur automatisé (2.16.124.113550.2.4.4.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = AIGCEV Authorize-use (1.3.6.1.4.1.51528.1.1) CPD = http://crl1.notarius.com/crl1-ca3/crl/notarius_certificate_authority_3_crlfull.crl SubjectAltName = URL=http://uri.aigcev.org/[unifromRessourceIdentifier]

- ***Profil Standard d'évaluation – ICA3***

Champ de base	Valeur

Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
Longueur des clés	ECC P-256
Durée de validité du certificat	6 mois à 10 ans
Extension du certificat	Certificate policies = Identity NOT verified / Identité NON vérifiée (2.16.124.113550.2.4.1.0) Legal person / Personne moral (2.16.124.113550.2.4.2.2) Software support / Support logiciel (2.16.124.113550.2.4.3.1) Intended for server automation / Pour serveur automatisé (2.16.124.113550.2.4.4.1) Intended for Adobe test / Pour test Adobe (1.2.840.113583.1.2.2) AIGCEV test-certificate (1.3.6.1.4.1.51528.2.1) Key usage = Signature numérique (2.5.29.15); Extended Key Usage = AIGCEV Authorize-use (1.3.6.1.4.1.51528.1.1) CPD = http://crl1.notarius.com/crl1-ca3/crl/notarius_certificate_authority_3_crlfull.crl SubjectAltName = URL=http://uri.aigcev.org/[unifromRessourceIdentifier]

7.2 Profil OCSP

Les profils OCSP décrivent :

- le format des réponses,
- les extensions obligatoires et optionnelles,
- les algorithmes de signature,
- les règles de fréquence de mise à jour et d'actualisation des statuts,
- les points de distribution OCSP associés à chaque AC.

Les paramètres décrits dans les tableaux sont conformes :

- à ETSI EN 319 411-1, clauses sur l'information d'état,
- au RFC 6960 (OCSP),
- au Mozilla Root Store Policy, incluant les exigences de fiabilité et de disponibilité.

L'AC Serveurs s'assure que les informations d'état publiées via OCSP sont cohérentes avec celles publiées dans les LCR correspondantes (voir section 5 et section 6).

Les réponses OCSP contiennent des dates de validité permettant à l'utilisateur d'établir sir

la réponse OCSP est assez récente pour l'usage qu'il souhaite en faire. Le répondeur OCSP utilise l'extension ArchiveCutOff telle que spécifiée dans la RFC 6960 de l'IETF, avec la date archiveCutOff fixée à la valeur de la date et de l'heure "notBefore" du certificat de l'AC.

- ***Profil du certificat d'OCSP – ICA1***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
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 = Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2); Intended for server automation / Pour serveur automatisé (2.16.124.113550.2.2.4.2); Key usage = Signature numérique (2.5.29.15); Extended Key Usage = Signature OCSP (1.3.6.1.5.5.7.3.9);
CDP	http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl
1.3.6.1.5.5.7.48.1.5	No Revocation Check

- ***Profil du certificat d'OCSP – ICA2***

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority 2 [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA

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 = Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.3.3.2); Intended for server automation / Pour serveur automatisé (2.16.124.113550.2.3.4.2); Key usage = Signature numérique (2.5.29.15); Extended Key Usage = Signature OCSP (1.3.6.1.5.5.7.3.9);
CDP	http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl
1.3.6.1.5.5.7.48.1.5	No Revocation Check

- ***Profil du certificat d'OCSP – ICA3***

s.o

7.3 Profil des LCR

Les LCR sont conformes à la norme X.509, version 3.
Si le PSC/R supprime de la LCR les certificats révoqués après leur expiration, la LCR n'inclura pas l'extension X.509 "ExpiredCertsOnCRL" telle que définie dans la norme ISO/IEC 9594-8/Recommandation ITU T X.509.
Si des LCR sont fournies et que Notarius décide ou est tenu de mettre fin à une LCR, il émettra et publiera au point de distribution de LCR correspondant une dernière LCR avec une valeur de champ nextUpdate telle que définie dans la norme ETSI EN 319 411-1 [2], clause 6.3.9. Exigence CSS-6.3.9-06 (La résiliation de la LCR peut se produire lorsqu'il n'y a plus de certificats valides dans la portée de la LCR, par exemple lorsque le certificat de l'entité de signature de la LCR expire ou lorsque la clé privée de l'entité de signature de la LCR est déclassée).
En cas de compromission de l'AC, Notarius diffusera une LCR sur l'état de révocation de l'AC avec le statut de révocation à jour sur les points de distribution déjà définis.
En cas de fin de vie de l'AC, la LCR émise par Notarius le sera avec un champs NextUpdate d'une valeur de 99991231235959Z.
Notarius n'émettra pas de dernière LCR avant que tous les certificats visés par cette LCR ne soient expirés ou révoqués.

- http://crl-ica1.certifio.com/notarius_certificate_authority_crlfull.crl

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

Champ de base	Valeur
Émetteur	CN = Notarius Certificate Authority O = Notarius Inc 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 =0e d0
Identificateur de clé de l'autorité	1d 5a 27 f6 e5 ac 17 84 6b d1 04 1e 84 ec d4 2c ad 3f d3 7f

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

Champ de base	*Valeur*
Émetteur	CN = Notarius Certificate Authority 2 O = Notarius Inc 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 =0d 4d
Identificateur de clé de l'autorité	ef f7 25 89 43 bf ac b7 a4 13 55 b3 ee b1 74 b6 02 6a 38 4b

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

Champ de base	Valeur
Émetteur	CN = Notarius Certificate Authority 3 O = Notarius Inc C = CA
Date d'entrée en vigueur	
Prochaine mise à jour	
Algorithme de signature	SHA256ECDSA
Algorithme de hachage de la signature	sha256
Numéro de la liste de révocation des certificats	Nombres de CRL = [nombre incrémental]
Identificateur de clé de l'autorité	1499b78f9ad1f7bb75506ed3fd32a13a0fd43fc3

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

Champ de base	*Valeur*
Émetteur	CN = Notarius Root Certificate Authority O = Notarius Inc C = CA
Date d'entrée en vigueur	5 septembre 2019 10:26:30
Prochaine mise à jour	16 décembre 2019 19:00:00
Algorithme de signature	sha256RSA
Algorithme de hachage de la signature	sha256
Numéro de la liste de révocation des certificats	Nombres de CRL =0b
Identificateur de clé de l'autorité	Identifiant de la clé=99 c9 10 4a 7d 78 ba 89 56 31 4e f5 ec 35 73 3d a4 1b ed 6e
Émission de point de distribution	Nom du point de distribution : Nom complet : Adresse d'annuaire : CN=CRL1 CN=Notarius Root Certificate Authority O=Notarius Inc C=CA URL=ldap://X1-PROD/cn=CRL1,cn=Notarius%20Root%20Certificate%20Authority,o=Notarius%20Inc,c=CA?authorityRevocationList?base URL=http://crl.notarius.com/notarius_root_ca/crl/crl_roota1.crl Ne contient que des certificats utilisateur=Non Ne contient que des certificats d'autorité de certification=Oui Liste de révocation des certificats indirects=Non

7.4 Profil TSA

Le profil TSA décrit :

- l'algorithme de signature utilisé par la TSA,
- les attributs de la signature d'horodatage,
- les OID de politique TSA (TimeStampPolicy),
- les paramètres techniques requis pour assurer la validité de l'horodatage.

Le service TSA est conforme aux exigences de l'ETSI EN 319 421 et utilise des clés et certificats émis par l'AC conformément à la CP pertinente et aux pratiques de sécurité

décrites dans la section 6.

Champ de base	Valeur
Issuer DN	cn=Notarius Certificate Authority [*incrémenté d'un chiffre au besoin*] o=Notarius Inc c=CA
Subject DN	cn=[nom du détenteur, du groupe ou du dispositif] uid =[identificateur unique] ou=[nom du RPR ou de l'entreprise] o= [nom du produit] c=CA
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 = Conforme à -Adobe Approved Trust List (AATL) (2.16.124.113550.2.2.4.2) Cryptographic support required / Support cryptographique requis (2.16.124.113550.2.2.3.2) Extended Key Usage = Tampon temporel (1.3.6.1.5.5.7.3.8) CPD = http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl Mail = Email
AIA	http://ocsp1.notarius.com/ocsp1-ca1 ou http://ocsp-ica1.certifio.com/ocsp

7.5 Notes générales sur les profils

Pour tous les certificats et services :

- Les longueurs de clés et algorithmes utilisés sont conformes au tableau des algorithmes (section 6).
- Les DN utilisés diffèrent selon l'AC, le type de certificat et les exigences contractuelles applicables.
- Les OID de politiques correspondent précisément aux CP distinctes propres à chaque AC (CCQ, ICA1, ICA2, ICA3).
- Aucun attribut de DN n'est utilisé sans justification opérationnelle ou normative.
- Les extensions critiques sont limitées à celles requises par les standards.
- Les horodatages OCSP et LCR respectent strictement la synchronisation NTP (voir section 6.8).

8 Audit de conformité et autres évaluations

Les audits et évaluations couvrent à la fois les contrôles requis pour l'obtention et le maintien des qualifications au sens du règlement eIDAS, ainsi que les contrôles réalisés périodiquement à l'initiative du PSC/R afin de s'assurer que l'ensemble des composantes de l'ICP demeure conforme :

- aux engagements publiés dans les CP,
- aux pratiques décrites dans la CPS,
- aux politiques de sécurité en vigueur,
- aux normes applicables (ETSI, ISO 27001, ISO 9001),
- et aux obligations légales et réglementaires pertinentes.

Ces activités visent à confirmer que les services de certification offerts respectent les exigences de sécurité, d'intégrité, de disponibilité et de conformité attendues d'une AC opérant sous un environnement de confiance réglementé.

8.1 Fréquence et/ou circonstances des évaluations

L'AC a la responsabilité du bon fonctionnement des composantes de l'ICP. Elle fera effectuer des contrôles internes réguliers de conformité et de bon fonctionnement des composantes de l'ICP.

- Avant la première mise en service d'une composante clé de l'ICP une cérémonie selon un processus encadré est réalisé. Un témoin externe est toujours présent et un compte-rendu détaillé est rédigé par l'Officier ICP.
- Tout changement important dans l'ICP est documenté dans une MEP (mise en production) incluant l'évaluation d'impact, les tests requis et l'approbation formelle.

Le PSC/R pourra également être soumis à des audits externes à la demande des ALE avec lesquels il a conclu une entente à cet effet, afin de valider la conformité des ANS, des clauses de l'Entente, de la CPS, de la CP et aux Politiques internes référées dans ces deux documents.

L'audit sera basé sur des informations opérationnelles et ne comprendra aucune information personnelle. Chacune des parties assumera les coûts de ses propres ressources.

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 & ETSI EN 319 412-3], ISO 27001 et ISO 9001.

8.2 Identités/Qualification des évaluateurs

Les contrôles sont effectués par une équipe d'auditeurs compétents en sécurité des systèmes d'information ou dans le domaine d'activité de la composante contrôlée.
Les auditeurs désignés peuvent être internes comme externes au PSC/R.
Si un auditeur interne n'est pas en mesure au 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.
Les 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.

À l'interne, le PSC/R a établi plusieurs procédures à suivre pour rencontrer ces exigences :

- Audit trimestriel de sécurité
- Audit des logs des PKI
- Procédure d'audits internes
- Procédure de gestion des NC/DAC/DAP
- Politique qualité
- Politique de sécurité

À l'externe, les auditeurs externes dûment autorisés à pratiquer les contrôles visés sont désignés par le PSC/R ou les partenaires d'affaires et doivent être indépendants de l'AC et du PSC/R. Avant l'exécution de leur mandat, des ententes contractuelles et des ententes de confidentialité doivent être signées.
Les auditeurs externes ne doivent appartenir ni à l'entité opérant la composante contrôlée, quelle que soit cette composante et, si l'AC entière est contrôlée, ni ne faire partie des divisions opérationnelles de l'AC.

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. Leur rôle est ajouté à leur description d'emploi.
Les auditeurs externes sont sélectionnés selon le processus de sélection des fournisseurs du PSC/R. Ils doivent être indépendants, impartiaux et libres de tout conflit d'intérêts vis-à-vis de l'AC ou du PSC/R. Leur mandat est encadré contractuellement.

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 CP, la CPS et les processus afférents.
Les contrôles sont annuellement planifiés. Ils peuvent être également ponctuels ou périodiques.
Lors d'un audit externe, l'ampleur des sujets ou des éléments à vérifier peut-être plus précise ou restreinte selon que l'audit en soit un de contrôle ou un de re-certification.
L'auditeur externe établira un programme d'audit préalable à sa venue permettant de définir précisément quelles composantes du service de certification sont visées par l'audit.
La Déclaration du champ d'application de la certification est retranscrite sur les certificats émis par l'auditeur externe après son audit.

8.5 Actions prises à la suite des conclusions des évaluations

À l'issue d'un audit externe, un rapport formel classé confidentiel est produit par l'auditeur externe du PSC/R faisant état notamment des non-conformités, des écarts mineurs et des

opportunités d'amélioration.
Le PSC/R doit corriger immédiatement les non-conformités et proposer un plan de résolution des écarts mineurs ou opportunités d'amélioration.
Les conclusions du rapport sont présentées lors de Comités dédiés.
Le traitement des non-conformités, des écarts mineurs et des opportunités d'amélioration est réalisé dans l'espace dédié de Podio.
Tout manquement identifié en dehors d'un audit peut être porté aux gestionnaires concernés, qui entreprennent les mesures appropriées.

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.
Les certificats de conformité ISO 9001, ISO 27001 et eIDAS délivrés à la suite des audits externes sont publiés sur le site Web du PSC/R et sont accessibles au public pour consultation.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Frais d'abonnement

Des frais peuvent être exigés pour l'abonnement à un produit de l'ICP de Notarius. Ces frais représentent ceux que l'Acheteur doit payer annuellement ou mensuellement, selon les cas, pour l'utilisation par un Détenteur d'un ou plusieurs produits de l'ICP, en sus des frais d'adhésion et des frais transactionnels.

Les frais sont facturés selon l'échelle tarifaire diffusée sur le site Web Notarius, ou selon les conditions négociées dans une entente contractuelle écrite.

Les conditions tarifaires en vigueur pour l'acquisition de certificats sont publiées sur le site web de Notarius.
La mise à jour des tarifs passe par le Comité ISO+ (PSC/R).

Après approbation de ce dernier, la mise à jour du site Web et du CRM le cas échéant est effectuée par l'équipe du Marketing, généralement via les processus internes (Podio).

Avant l'entrée en vigueur de nouveaux tarifs, le PSC/R s'engage à notifier ses clients et partenaires concernés au moins 30 jours à l'avance.

Les ententes contractuelles particulières peuvent limiter ou encadrer les augmentations.

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 pourraient 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 devra être préalablement conclut 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 pourraient être facturées à l'Acheteur.

9.1.4 Tarifs pour d'autres services

D'autres services pourraient être facturés, notamment des frais d'utilisation déraisonnable des produits. Dans ce cas, ces tarifs seront portés à la connaissance des personnes auxquelles ils s'appliquent.
Également le PSC/R pourrait exiger des frais pour :

- Une demande de réémission d'un certificat;
- Le renouvellement des clés et des certificats;
- La révocation d'un certificat.

9.1.5 Politique de remboursement

Dans le respect des conditions générales d'utilisation, Notarius ne remboursera à l'Acheteur que les Frais d'Abonnement qui répondent aux exigences suivantes : (i) dans le cas où un Regroupement de Professionnels ou encore un employeur refuse une demande d'Abonnement à un ou des Produits; ou (ii) si le Détenteur n'est pas en mesure d'installer les applications nécessaires à l'activation de sa Signature numérique.
Tous les autres frais et paiements ne sont ni remboursables, ni annulables, ni objet d'un crédit en cours d'Abonnement, incluant notamment le cas où le Détenteur n'est plus membre de son Regroupement de Professionnels.

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, certaines ententes contractuelles peuvent 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 et adaptée aux technologies de l'information.
Les contrats d'assurances sont classés dans un répertoire dédié du PSC/R.
Également une copie du certificat d'assurance incluant les limites de responsabilité des montants d'assurances peut être remis sur demande écrite au responsable identifié à la section 1.8.2 des présentes.

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;

- 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;
- Les causes de révocation, sauf accord explicite de publication de l'ALE;
- Les informations techniques relatives à la sécurité des fonctionnements de certaines composantes de l'ICP et de son infrastructure.

Le PSC/R, les ALE, les AVI et les AVA prennent les mesures nécessaires pour protéger les informations confidentielles qu'ils détiennent.
Ces informations confidentielles ne sont utilisées et ne font l'objet d'aucune communications extérieures que :

- Lors de l'exécution des prestations de services de certification définies dans le présent document ;
- Pour répondre aux exigences légales ;
- Pour l'exécution de travaux ou de prestations de services de certification confiés à un fournisseur de services autorisé par le PSC/R;
- Lors de la cessation des activités du PSC/R. Un accord de transfert des données personnelles devra alors être obtenu par le PSCR/R pendant la durée du préavis.

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* (L.R.Q, 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 personnelles

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 au Canada et au Québec.

9.4.5 Notification et consentement d'utilisation des données personnelles

Les informations personnelles données 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 sa Politique de confidentialité.

9.4.6 Divulgation aux autorités

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 divulgations

Sans d'engagement spécifique.

9.5 Propriété intellectuelle

Solutions Notarius inc. détient tous les droits de propriété intellectuelle sur la CP, la CPS, les applications et les infrastructures technologiques de l'ICP.
Les cabinets dans lesquels sont entreposées les infrastructures technologiques situées au site de production et de relève sont loués à des entreprises spécialisées dans le domaine et répondant à de hauts critères de sécurité (voir les contrats de colocation).

Les détenteurs détiennent les droits relatifs à leurs renseignements personnels apparaissant sur les certificats, sans toutefois détenir la propriété du certificat lui-même (droit d'usage uniquement).

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.

La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou

partielle, par quelque moyen que ce soit, notamment, électronique, mécanique, optique, photocopie, enregistrement informatique, des éléments mentionnés dans la présente CPS est strictement interdit sans autorisation écrite préalable.

Les marques Notarius[MD] et CertifiO[MD], sont des marques déposées de Solutions Notarius Inc.
Toute reproduction ou utilisation de ces marques sans autorisation préalable écrite de Solutions Notarius Inc., est interdite.

9.6 Interprétations contractuelles et garanties

9.6.1 Relativement aux renseignements inscrits au certificat

Le PSC/R s'assure que les renseignements inscrits obligatoirement aux certificats sont conformes aux données vérifiées et confirmées par l'AVI et/ou l'AVA, selon la procédure prévue pour le niveau de confiance du produit/type de certificat.

9.6.2 Relativement aux renseignements inscrits au répertoire

Le PSC/R doit s'assurer de l'exactitude des LCR inscrites au répertoire.

9.7 Limite de garantie

Les limites de garantie sont exprimées dans les conditions générales d'utilisation de Notarius à la section limitation de garantie et de responsabilité.

9.8 Limite de responsabilité

À moins d'entente contractuelle particulière, les limites de responsabilité sont exprimées dans les conditions générales et particulières d'utilisation des produits de Notarius.
Sous réserve des dispositions d'ordre public applicables, l'AC et le PSC/R ne peuvent être tenues responsables d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LCR, des LAR ainsi que de tout autres équipement ou logiciel mis à la disposition des détenteurs de certificats.

Le PSC/R décline sa responsabilité notamment pour tout dommage résultant :

- Des erreurs ou des inexactitudes entachant les renseignements contenus dans les certificats résultant des informations provenant du tiers ayant effectué les vérifications;
- De l'utilisation des clés et des certificats pour un usage autre que ceux prévus à la CP ou expressément spécifié au contrat d'adhésion;
- De l'usage d'un certificat révoqué ou expiré;
- Des certificats portant la mention « certificat de test » ou toute autre mention de même nature indiquant qu'on ne peut raisonnablement s'y fier;
- De l'absence de révocation d'un certificat entraînant l'utilisation du certificat par

un tiers non autorisé;
- D'un cas de force majeure.

Les détenteurs de certificat doivent se conformer à toutes les exigences de la CP et de la présente CPS ainsi qu'aux termes et conditions des produits qu'ils ont achetés.

9.9 Indemnisation

À moins d'Entente contractuelle particulière, les cas d'Indemnisation sont exprimés dans les conditions générales d'utilisation des produits de Notarius.

9.10 Procédures d'approbation

9.10.1 Approbation de la CP

Lorsque la CP est modifiée, elle doit être soumise pour approbation au CEO de l'AC.
L'AC avise le PSC/R de toute modification entraînant des changements à la CPS et, en cas d'impacts sur les procédures, lui accorde un délai raisonnable pour 'y conformer.
Une fois les modifications approuvées, elle est publiée sur le site web de l'AC dans un délai raisonnable.

9.10.2 Approbation de la CPS

La CPS respecte la CP.
Les modifications apportées à la CPS, sont approuvées par le Comité ISO+ du PSC/R et l'AC est avisée.

9.10.3 Durée et validité

La CPS est valable jusqu'à ce qu'elle soit remplacée par une nouvelle version ou jusqu'à ce que l'AC cesse ses activités.
La fin de validité de la CPS met également fin à toutes les clauses qui la composent.
Sauf évènement exceptionnel directement lié à la sécurité, les nouvelles versions de la CP et de la CPS n'imposent pas la révocation des certificats déjà émis.

9.11 Avis individuels et communications avec les participants

En cas de changement majeurs à intervenir dans les composantes de l'ICP, le RSI du PSC/R analysera l'impact de tels changements en termes de sécurité et de qualité des services offerts.
Des analyses de risques seront alors ouvertes et détaillées dans Podio

9.12 Amendements

Le PSC/R veille à s'assurer que tout changement apporté à la CPS reste conforme aux lois, règlements et exigences de certification.
Toutes les nouvelles versions de la CPS seront déposées sur le site Web de l'AC.

9.13 Résolution des conflits

Les plaintes sont reçues via les canaux habituels du Support de Notarius par clavardage, courriel ou téléphone. Elles sont documentées dans l'outil de billetterie, prises en charge, évaluées et traitées selon la procédure interne. En cas de contestation ou de litige, résultant du non-respect d'obligations contractuelles intervenues entre le PSC/R et les ALE chaque partie devra aviser par écrit le département chargé de recevoir les notification par courrier électronique identifié dans l'entente en litige. La date réputée de réception de tout avis donné sera le lendemain du jour de l'envoi de la transmission courriel.

Le règlement des différends est détaillé dans les conditions générales d'utilisation des produits de Notarius.

À moins d'entente contractuelle contraires, tout conflit découlant des services de l'ICP doit être prioritairement réglé par la négociation de bonne foi.
Les litiges contractuels sont soumis au processus de notification, puis :

- Négociation de bonne foi (15 jours)
- Médiation (Centre canadien d'arbitrage commercial)
- Arbitrage (final et sans appel)

L'arbitrage est confidentiel et tenu à Montréal.

Par souci de clarté, rien dans les présentes n'empêchera une Partie de demander une mesure injonctive si elle estime que, sans une telle mesure, un préjudice grave pourrait lui être causé.
L'application de la Convention des Nations unies sur les contrats de vente internationale de marchandise est expressément exclue.

9.14 Juridictions compétentes

La présente CPS est régie et interprétée conformément aux lois applicables dans la Province de Québec, et les lois fédérales canadiennes applicables dans cette province, sans donner effet aux conflits de lois.

9.15 Interprétation

9.15.1 Lois et règlements applicables

Les lois et règlements applicables sont notamment :

- Loi concernant le cadre juridique des technologies de l'information (LCCJTI)
- La Loi sur protection des renseignements personnels dans le secteur privé
- Code civil du Québec (L.Q., 1991, c.64), notamment les articles 36 et 37, qui portent respectivement sur le respect de la vie privée et la communication des renseignements confidentiels;
- Code criminel du Canada (L.R.C., 1985, c. C-46), notamment les articles 342.1, 366 et 430, qui portent respectivement sur l'interception frauduleuse d'informations, la falsification des documents et les méfaits;
- Loi sur le droit d'auteur (L.R.C., 1985, c. C-42);
- Loi sur les marques de commerce (L.R.C., 1985, c. T-13);

- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);
- Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12) et la Charte canadienne des droits et libertés, Annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R-U);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1);
- Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., c. P-39.1)
- Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, c. 5);
- Loi sur les archives (L.R.Q., c. A-21.1), en ce qui a trait aux exigences relatives à la protection et à la conservation des documents ayant une valeur patrimoniale ou archivistique;
- Code des professions (L.R.Q., c. C-26)

9.15.2 Indépendance des dispositions

Le fait pour une ou plusieurs dispositions de la CPS d'être déclarées invalides, illégales ou inapplicables ne porte pas atteinte à la validité des autres dispositions.
La CPS continuera donc à s'appliquer en l'absence de la disposition inapplicable tout en respectant l'intention des parties concernées.

9.16 Force majeure

La force majeure est un évènement extérieur, imprévisible, irrésistible et incontrôlable qui rend impossible la réalisation d'une obligation.
Sont considérés comme des cas de force majeure tous ceux habituellement retenus par les tribunaux canadiens et plus spécifiquement ceux issus de la définition qui est donnée de cette expression à l'article 1470 du Code civil du Québec.

9.17 Revue

La CPS est revue et republiée annuellement pour donner suite à la révision de la CP ou des processus internes de Notarius. Une nouvelle date et un nouveau numéro de version seront alors appliqués.

9.18 Entrée en vigueur

La CPS entre en vigueur à la date de son adoption par le Comité ISO+ de Solutions Notarius Inc.