CAHIER DE CHARGES

Règlement sur la signature officielle numérique du notaire, RLRQ, c. N-3, r. 13.1

Direction Secrétariat, Services juridiques, Relations institutionnelles et Gouvernance

Version: 17 décembre 2020

100-2045, rue Stanley, Montréal QC H3A 2V4
Tél. : 514-879-1793 / 1-800-263-1793
www.cnq.org

Historique des versions

Date	Version	Description	Auteur
17/12/2020	v. 1.0	Version finale pour publication sur le site Internet de l'Ordre.	Catherine Bolduc

Approbation du livrable

Date	Approbateur	Livrable	Résolution
27/03/2020	Conseil d'administration	Orientations présentées au cahier de charges pour les prestataires de services de signature officielle numérique, telles qu'énoncées aux termes du document AD-2546a.	CAD-50-35-6.3
17/12/2020	Brunelle, Stéphane Directeur général	v. 1.0	Pouvoirs conférés par CAD-50-35-6.3

TABLE DES MATIÈRES

Objectif du cahier de charges

Le notaire qui signe un acte notarié doit utiliser sa signature officielle. Il peut également apposer sa signature officielle sur tout document qu'il est appelé à signer dans l'exercice de sa profession.

Cette signature officielle est écrite ou apposée au moyen d'un procédé technologique.

L'objectif de ce cahier de charges est d'énoncer les conditions, modalités et autres exigences qu'un prestataire de services de certification devra remplir afin de conclure une entente avec la Chambre des notaires du Québec lui permettant d'être autorisé à délivrer une signature officielle apposée au moyen d'un procédé technologique. Il découle du *Règlement sur la signature officielle numérique du notaire*[1] (le « **Règlement** »), entré en vigueur le 1er décembre 2019.

Mises en garde

1. Le prestataire de services de certification intéressé à offrir sa solution de signature officielle numérique aux notaires doit d'abord évaluer avec les fournisseurs concernés la possibilité que soit intégrée cette dernière aux solutions métier couramment utilisées par les notaires.

Mentionnons les solutions métier suivantes :

Fournisseur	Solution métier	Description
Chambre des notaires	InscriptiO	Publication électronique des rapports de dispositions testamentaires, de mandats de protection et de consentements au don d'organes et de tissus auprès des registres du même nom.
Chambre des notaires	Recherche électronique registres	Recherche électronique de dispositions testamentaires et de mandats de protection dans les registres du même nom.
Acceo Solutions inc.	ProNotaire	Logiciel de gestion d'étude notariale permettant la publication électronique d'actes au Registre foncier du Québec ainsi que la publication électronique des rapports de dispositions testamentaires, de mandats de protection et de consentements au don d'organes et de tissus auprès des registres du même nom.
Acceo Solutions inc.	ProCardex	Logiciel de gestion d'étude notariale permettant la publication électronique d'actes au Registre foncier du Québec ainsi que la publication électronique des rapports de dispositions

[1] RLRQ, c. N-3, r. 13.1

Fournisseur	Solution métier	Description
		testamentaires, de mandats de protection et de consentements au don d'organes et de tissus auprès des registres du même nom.
Avancie inc.	Para-Maître	Logiciel de gestion d'étude notariale permettant la publication électronique d'actes au Registre foncier du Québec ainsi que la publication électronique des rapports de dispositions testamentaires, de mandats de protection et de consentements au don d'organes et de tissus auprès des registres du même nom.
Ministère de l'Énergie et des Ressources naturelles du Québec	Service en ligne de réquisition d'inscription ou SLRI	Publication électronique d'actes au Registre foncier du Québec.
Telus	Assyst Immobilier	Portail sécurisé de traitement des mandats hypothécaires par Internet permettant des échanges de fichiers sur les clients entre les notaires et les institutions financières au Canada.
Telus	Assyst Paiement	Solution qui permet aux notaires de transmettre et recevoir des fonds sous forme de paiement électronique.

2. Les exigences prévues au présent cahier de charges pourraient nécessiter des ajustements selon la nature et les fonctionnalités de la solution de signature officielle numérique proposée par le prestataire de services de certification. Cependant, il va de soi qu'il ne sera pas possible de déroger à toute exigence prévue au Règlement.

3. Le prestataire de services de certification devra effectuer un banc d'essai de sa solution à la Chambre des notaires avant que ne soit entrepris le processus d'autorisation. L'objectif du banc d'essai est de démontrer la réponse aux exigences prévues au cahier de charges. Le banc d'essai permettra également de prévoir les adaptations qui peuvent être requises aux façons de faire des notaires.

4. Un audit en vertu du Bloc 7 devra être réalisé avant la signature de l'Entente.

Définitions

Les mots et expressions qui suivent ont, sauf si le contexte le requiert autrement, le sens qui leur est ci-après donné et ce, indépendamment du fait qu'ils débutent ou non par une lettre majuscule :

- « **AC** » signifie autorité de certification.
- « **AVA** » signifie agent de vérification de l'affiliation professionnelle.

- « **Chambre** » signifie Chambre des notaires du Québec.
- « **Canal de communication** » signifie le ou les moyens de communication sécuritaires exploités par le Prestataire, à ses frais, permettant l'échange entre ce dernier, la Chambre et le notaire de renseignements, notamment sur les Demandes d'autorisation et les Révocations des clés et des certificats.
- « **Contrat de service** » signifie le contrat de fourniture de la Solution au notaire par le Prestataire, incluant ses conditions d'utilisation.
- **« CPS »** signifie « Certification Practice Statement » ou « Énoncé des pratiques de certification », soit le document définissant les processus et les pratiques opérationnelles qui seront utilisés pour maintenir le niveau de service convenu et satisfaire aux exigences de sécurité pour une infrastructure à clés publiques, ceci afin de prouver que les certificats délivrés sont valides et dignes de confiance. Le Prestataire doit démontrer le respect du CPS de son infrastructure à clés publiques lors d'un audit.
- « **Demande d'autorisation** » signifie la demande formulée par le notaire à la Chambre dans le but d'être autorisé à utiliser une SON.
- « **Document technologique** » signifie un document échangé, généré, produit, conservé ou transmis par un notaire de quelque manière qu'il soit et dont le support fait appel aux technologies de l'information, au sens de la *Loi concernant le cadre juridique des technologies de l'information*[2], incluant toutes données, banques de données et métadonnées sous-jacentes qui en permettent la création. À titre d'exemple, il peut s'agir de renseignements confidentiels, de renseignements personnels au sens des lois applicables en l'espèce, d'informations sur les clients, de courriels, de contrats ou d'ébauches d'avis juridique. Le Document technologique appartient au notaire.
- « **Entente** » signifie l'entente qui doit être signée entre le Prestataire et la Chambre en vertu de l'article 6 du Règlement.
- « **LCR** » signifie liste des certificats révoqués.
- « **NAVI** » signifie notaire agent vérificateur d'identité.
- « **Partenaire** » signifie indistinctement tout mandataire, sous-traitant, consultant, partenaire d'affaires, revendeur, prestataire de services ou entrepreneur du Prestataire, ainsi que les partenaires de ces derniers.
- « **PC** » signifie politique de certification.

[2] RLRQ, c. C-1.1

- « **Prestataire** » signifie l'AC, le PSC/R ou les deux.[3]
- « **PSC/R** » signifie prestataire de services de certification et de répertoires.
- « **Responsables Chambre** » désigne les personnes AVA déterminées par la Chambre qui seront responsables des communications avec le Prestataire et des opérations courantes de la Chambre relatives à l'utilisation de la Solution par les notaires.
- « **Responsables Prestataire** » désigne les personnes désignées par le Prestataire qui seront responsables des opérations courantes du Prestataire dans l'exploitation de la Solution et des communications entre le Prestataire et le Chambre.
- « **Révocation d'autorisation** » signifie la révocation d'une Demande d'autorisation délivrée par la Chambre dans les cas prévus par l'article 4 du Règlement. Elle entraîne automatiquement une Révocation des clés et des certificats.
- « **Révocation des clés et de certificats** » signifie la révocation de la SON d'un notaire par le Prestataire.
- « **SMSI** » signifie système de management de la sécurité de l'information. Défini ainsi dans la norme ISO/IEC 27001:2013 : « Un SMSI se compose des politiques, procédures, lignes directrices et des ressources et activités associées, gérées collectivement par un organisme dans le but de protéger ses actifs informationnels. Un SMSI utilise une approche systématique visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, maintenir et améliorer la sécurité de l'information d'un organisme afin que celui-ci atteigne ses objectifs métiers. Cette approche se fonde sur l'appréciation du risque et sur les niveaux d'acceptation du risque définis par l'organisme pour traiter et gérer efficacement les risques. L'analyse des exigences de protection des actifs informationnels et l'application des mesures appropriées pour assurer, comme il se doit, la protection de ces actifs, contribuent à la réussite de la mise en œuvre d'un SMSI. »
- « **Solution** » signifie la solution du Prestataire incluant le procédé technologique permettant d'apposer une signature officielle numérique au sens du Règlement.
- « **SON** » signifie signature officielle numérique.
- « **VI** » signifie vérification d'identité.

[3] Les parties et intervenants à l'Entente, dont le Prestataire, seront déterminés en fonction des entités en présence et de la façon dont la Solution est exploitée par elles. Ainsi, l'AC et le PSC/R pourraient ne pas être les seuls à être soumis aux exigences du cahier de charges et l'Entente pourrait comporter d'autres signataires.

Bloc 1 : Exigences relatives au Prestataire

Le Prestataire doit satisfaire aux exigences énoncées dans la grille suivante.

Nº	Bloc 1 : Exigences	Motif / précision
1.	Le Prestataire a la solidité financière lui permettant de faire face à ses obligations et suivre l'évolution des technologies.	Au moment de la conclusion de l'Entente et à tous les 3 ans de la date anniversaire de la signature de l'Entente, le Prestataire devra fournir une lettre de confort d'un tiers auditeur, en plus de démontrer qu'il n'est pas en faillite et qu'il n'a pas fait de proposition concordataire. Dans certains cas, une garantie pourrait être exigée d'un tiers.
2.	Le Prestataire est incorporé en vertu d'une loi canadienne ou de la loi d'une province canadienne.	
3.	Le Prestataire est immatriculé au Registraire des entreprises du Québec ou, alternativement, il a désigné un fondé de pouvoir au Québec.	
4.	Le Prestataire est inscrit au Registraire des entreprises du Québec ou à Corporation Canada et son état des renseignements ne révèle aucune non-conformité.	
5.	Le Prestataire, ainsi que ses actionnaires, administrateurs, dirigeants, associés, employés et Partenaires, ne figurent pas et n'ont jamais figuré au Registre des entreprises non admissibles aux contrats publics (RENA).	
6.	Le Prestataire, ainsi que ses actionnaires, administrateurs, dirigeants, associés, employés et Partenaires, sont honnêtes et intègres.	Les "Déclarations, garanties et engagements" signés par le Prestataire accompagnent sa demande de conclusion d'une Entente. Elles sont également fournies tous les ans à la date anniversaire de signature de l'Entente. (Voir Bloc 8)

Nº	Bloc 1 : Exigences	Motif / précision
7.	Le Prestataire exploite au Canada (idéalement au Québec) l'entreprise qui fournit la Solution depuis au moins 3 ans.	Une déclaration écrite du Prestataire à cet effet accompagne sa demande de conclusion d'une Entente.
8.	La Solution est exploitée en mode production depuis au moins 1 an.	Une déclaration écrite du Prestataire à cet effet accompagne sa demande de conclusion d'une Entente.

Bloc 2 : Conformité au Règlement sur la signature officielle numérique du notaire

La Solution devra satisfaire à toutes les conditions minimales prévues par le **Règlement sur la signature officielle numérique du notaire**.

Note: Certains des éléments de ce Bloc recoupent ceux du Bloc 4 Exigences de sécurité.

Nº	Bloc 2 : Conditions minimales	Référence au Règlement
1.	La Solution consiste en un système de cryptographie asymétrique supporté par une infrastructure à clés publiques qui permet d'apposer une SON.	Article 2
2.	Le Prestataire a une PC qui satisfait aux documents RFC 3647 et RFC 3280 élaborés par l'Internet Engineering Task Force et qui comprend une procédure de vérification de l'identité par un autre notaire.	Article 3, alinéa 2 et article 6, paragraphe 1 de l'alinéa 1
3.	Le Prestataire a un répertoire de certificats qui satisfait à la norme X.500 de l'Union internationale des télécommunications (UIT).	Article 6 paragraphe 3 de l'alinéa 1
4.	Le Prestataire délivre des certificats qui respectent la norme X.509 de l'UIT.	Article 6 paragraphe 4 de l'alinéa 1

Nº	Bloc 2 : Conditions minimales	Référence au Règlement
5.	Le Prestataire délivre des clés qui sont constituées d'une paire unique et indissociable, l'une publique et l'autre privée, qui permettent de signer un Document technologique et d'identifier le signataire.	Article 6 paragraphe 5 de l'alinéa 1
6.	Le Prestataire délivre des certificats qui comportent notamment les éléments suivants : a) le nom distinctif du notaire auquel est joint un code unique; b) la mention qu'il est notaire.	Article 2 Article 6 paragraphe 6 de l'alinéa 1 Le code de notaire sert de code unique. Le Prestaire ne peut émettre et activer qu'une seule SON par notaire. Une signature numérique autre qu'une SON émise par le Prestataire au notaire ne sera pas officielle : le certificat ne comportera pas la mention du fait qu'il est notaire.
7.	Le Prestataire inscrit les certificats dans un répertoire tenu sur un support faisant appel aux technologies de l'information et le met à jour. Ce répertoire contient, notamment, les numéros de série des certificats valides, suspendus, annulés ou archivés.	Article 6 paragraphe 7 de l'alinéa 1
8.	Le niveau de certification de la SON mis en œuvre par le Prestataire correspondra minimalement au niveau moyen-élevé : l'identité du notaire sera vérifiée par un autre notaire et le certificat sera stocké sur support logiciel. Toutefois, le stockage sur un dispositif protégé (jeton USB cryptographique, carte à puce) est nettement favorisé.	
9.	Le mécanisme d'activation des clés et des certificats et celui d'apposition de la SON doivent assurer que la clé privée est en tout temps sous le contrôle exclusif du notaire.	

Bloc 3 : Modalités administratives

Les modalités administratives suivantes seront convenues entre la Chambre et le Prestataire :

Nº	Bloc 3 : Modalités administratives	Motif / Précision / Article du Règlement
1.	Toutes demande, autorisation, refus, révocation, communication, avis entre le Prestataire, la Chambre et le notaire, requis dans l'exploitation courante de la Solution, devront s'effectuer au moyen du Canal de communication.	Le service à la clientèle (« help desk ») dispose d'un système de numérotation des communications journalisé.
2.	La Demande d'autorisation s'effectue sur le document établi par la Chambre.	Article 3, alinéa 1. Les alinéas 2 et 3 de l'article 3 du Règlement précisent les engagements des notaires qui doivent se trouver dans la Demande d'autorisation.
3.	La VI du notaire par un NAVI est obligatoire à l'obtention de l'autorisation à utiliser une SON par la Chambre. Une attestation de la VI est jointe à la Demande d'autorisation.	Article 3, alinéa 2
4.	Le Prestataire doit s'assurer, avant d'émettre une SON, que la Demande d'autorisation a été approuvée par la Chambre.	Article 3, alinéa 1 Article 7
5.	La Demande d'autorisation est approuvée ou refusée par la Chambre dans les 5 jours ouvrables suivant sa réception ou, selon le cas, dans les 5 jours ouvrables suivant le paiement à la Chambre des frais y relatifs.	
6.	Le notaire et le Prestataire sont avisés de l'approbation d'une Demande d'autorisation par la Chambre au plus tard le jour ouvrable suivant.	
7.	Le Prestataire doit transmettre au notaire les renseignements requis pour l'activation de sa SON au plus tard le jour ouvrable suivant la réception de l'avis d'approbation de la Chambre.	

Nº	Bloc 3 : Modalités administratives	Motif / Précision / Article du Règlement
8.	Le Prestataire informe immédiatement la Chambre et le notaire de la connaissance d'un cas de Révocation d'autorisation prévu à l'article 4.	Article 8
9.	À moins de circonstances exceptionnelles, la Révocation d'autorisation pour un des motifs prévus à l'article 4 du Règlement (à l'exception de celle découlant du décès du notaire) est effectuée par la Chambre dans le prochain jour ouvrable. En cas de circonstances exceptionnelles, ce délai est allongé d'un jour ouvrable.	
10.	La Révocation d'autorisation à la suite du décès du notaire est effectuée par la Chambre dans le jour ouvrable suivant celui de sa connaissance du décès.	
11.	La Révocation d'autorisation est immédiatement communiquée au Prestataire et au notaire.	Article 4, alinéas 1 et 2 Article 9, alinéa 1 *in fine*
12.	Le Canal de communication permet au notaire de procéder lui-même, auprès du Prestataire, à une Révocation immédiate des clés et des certificats.	
13.	La Révocation des clés et des certificats par le Prestataire est effectuée dans un délai maximal de 24 heures suivant la réception de la Révocation d'autorisation de la part de la Chambre.	
14.	La LCR et tout autre mécanisme de validation des clés et des certificats sont ajustés par le Prestataire au maximum dans les 5 minutes qui suivent une Révocation des clés et des certificats.	

Nº	Bloc 3 : Modalités administratives	Motif / Précision / Article du Règlement
15.	Le Prestataire informe la Chambre et le notaire d'une Révocation des clés et des certificats, même lorsqu'elle émane du notaire lui-même, dans les 5 jours ouvrables suivant cette Révocation.	Article 9
16.	Au moins un Responsable Chambre et au moins un Responsable Prestataire sont disponibles durant les jours ouvrables, aux fins de satisfaire aux exigences des modalités administratives.	Une Demande d'autorisation, une Révocation d'autorisation et une Révocation des clés et des certificats doivent pouvoir s'effectuer dans un contexte d'urgence, notamment en cas de compromission.
17.	Le service à la clientèle est disponible en français et en anglais.	
18.	Toute documentation afférente à la Solution est disponible en français.	
19.	La Solution est disponible 24h sur 24, 7 jours sur 7, 365 jours par année, à l'exception des périodes d'entretien.	Le notaire doit pouvoir utiliser sa SON en tout temps.
20.	Le Canal de communication doit être accessible à la Chambre et aux notaires 24h sur 24, 7 jours sur 7, 365 jours par année, à l'exception des périodes d'entretien.	Le notaire qui souhaite révoquer lui-même sa SON doit pouvoir le faire en tout temps, surtout si sa décision est motivée par une possible compromission. La Chambre peut également vouloir effectuer une Révocation d'autorisation en dehors des heures normales d'affaires, pour les mêmes raisons.
21.	Le Canal de communication permet au notaire d'aviser *immédiatement* la Chambre et le Prestataire en cas de compromission ou de motifs raisonnables de croire à une compromission de la SON.	Article 3, alinéa 4
22.	Le Prestataire doit disposer d'un processus de traitement des plaintes.	

Nº	Bloc 3 : Modalités administratives	Motif / Précision / Article du Règlement
23.	Le Prestataire doit disposer d'un processus de gestion des mauvais payeurs.	La Chambre n'interviendra pas dans ce processus. Elle s'exécutera sur simple demande du Prestataire de procéder à la Révocation d'autorisation au motif de défaut pour le notaire d'acquitter les frais relatifs à l'utilisation de sa SON.
24.	La PC, la CPS, le Contrat de service, la tarification, les niveaux de services et le processus de traitement des plaintes sont accessibles à la Chambre et aux notaires en tout temps, sur le Canal de communication.	
25.	Le fournisseur doit être doté d'un plan de continuité de service qui permet d'offrir un niveau de service acceptable pour les notaires (voir la ligne 17 de la Grille #1 de l'annexe). Le niveau de service jugé acceptable par la Chambre est le suivant: - lors d'une panne, le temps d'interruption admissible est de 4 heures; - lors d'un désastre majeur chez le fournisseur, le temps d'interruption admissible est de 72 heures.	
26.	Aucuns frais ne sont exigibles de la Chambre pour la mise en place et l'exploitation de la Solution et du Canal de communication par le Prestataire	
27.	Le Prestataire fournit gratuitement 5 SON à la Chambre.	Pour la gestion des Demandes d'autorisation et Révocations d'autorisation ainsi que pour des tests.
28.	La Chambre se réserve le droit de charger des frais au Prestataire pour la validation du respect des conditions minimales, modalités administratives, sécurité et les négociations et opérations relatives à l'Entente.	

Bloc 4 : Sécurité de l'information

Le Prestataire doit se conformer à la norme ISO/IEC 27001:2013 pour garantir une gestion maîtrisée de la sécurité de l'information avec un SMSI.

Le Prestataire et la Solution doivent satisfaire aux exigences du Bloc 4 et aux deux grilles d'exigences en annexe de ce cahier de charges.

Nº	Bloc 4 : Exigences de sécurité	Motif / précision
1.	Le Prestataire doit fournir une liste des coordonnées des Partenaires ou des sous-traitants directement affectés à la prestation du service de certification et de répertoire ainsi que ceux qui ont accès aux Documents technologiques du notaire, le cas échéant.	
2.	L'hébergement, la sauvegarde et la relève des Documents technologiques doivent s'effectuer en sol canadien.	
3.	La longueur des clés de chiffrement de la Solution, le cas échéant, doit satisfaire aux exigences du marché pour un chiffrement robuste des Documents technologiques.	Les clés de chiffrement doivent avoir une longueur de 2048 bits ou plus (année 2020) et des algorithmes appropriés selon les recommandations des autorités gouvernementales compétentes en la matière[4].
4.	Dans la mesure où la Solution permet au notaire de chiffrer ses Documents technologiques, le Prestataire prévoira une méthode de recouvrement des clés de chiffrement.	Nécessaire pour assurer la disponibilité des Documents technologiques, notamment auprès du syndic.

[4] Le Centre de la sécurité des télécommunications du gouvernement du Canada, une des organisations formant désormais le Centre canadien pour la cybersécurité, a publié des recommandations sur le chiffrement. Ces recommandations constituent une référence pour déterminer des exigences de nature cryptographique. L'hyperlien pointe sur le document *"Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)"* : https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b, consulté le 25 novembre 2020.

Bloc 5 : Garanties

Le Prestataire doit accorder les garanties suivantes à la Chambre aux termes de l'Entente.

Nº	Bloc 5 : Garanties	Motif / Précision/Article du Règlement
1.	Le Prestataire s'engage à implanter toute modification ultérieure aux conditions minimales prévues aux paragraphes 1, 3 et 4 de l'alinéa 1 de l'article 6 du Règlement.	Article 6 paragraphe 2 Le délai d'implantation est fixé à un an. Le Prestataire doit proposer un plan d'implantation et cette implantation fait l'objet d'un audit.
2.	Le Prestataire fournit en tout temps la plus récente version de la Solution, incluant les plus récentes mises à jour.	
3.	Le Prestataire se conforme en tout temps aux normes de sécurité qui lui sont applicables en fonction de ce qui a été déterminé au Bloc 4 : Sécurité et à l'annexe de ce cahier de charges.	Le Prestataire doit maintenir sa conformité au fil du temps en fonction de l'évolution des normes déterminées au Bloc 4.
4.	Le Prestataire est responsable des actes des Partenaires avec lesquels il transige dans le développement, l'exploitation, le maintien, l'entretien et l'évolution de la Solution.	
5.	Toute modification à la PC et au Contrat de service, touchant les notaires, doit faire l'objet d'un préavis écrit du Prestataire à la Chambre, 90 jours avant son entrée en vigueur.	
6.	Le Prestataire s'engage à défendre et à indemniser la Chambre et le notaire à l'égard de toute réclamation contre eux, dans la mesure où elle résulte de (i) l'exploitation de la Solution par le Prestataire et/ou ses Partenaires; ou (ii) découle de toute violation par le Prestataire des termes de l'Entente.	

Nº	Bloc 5 : Garanties	Motif / Précision/Article du Règlement
7.	Le Prestataire ne peut pas s'exonérer de sa responsabilité envers la Chambre.	
8.	Le Prestataire ne peut exclure ni limiter sa responsabilité envers le notaire (i) pour les réclamations d'un tiers alléguant une violation de droits de propriété intellectuelle; (ii) pour les dommages attribuables à ses manquements faisant l'objet d'engagements d'indemnisation exprès; ni (iii) pour les dommages attribuables à ses manquements aux obligations relatives à la sécurité de l'information.	
9.	En plus des autres garanties du Prestataire applicables au notaire et prévues au Bloc 5, le Contrat de service prévoira : (i) le cas échéant, la remise des Documents technologiques du notaire lors de la résiliation du Contrat, sur simple demande, moyennant des frais raisonnables dont le non-paiement ne peut servir à retenir ou retarder la remise, empêchant ainsi le notaire de poursuivre ses activités; (ii) la reconnaissance expresse par le notaire de l'absence de responsabilité de la Chambre pour tout manquement attribuable au Prestataire;	

Nº	Bloc 5 : Garanties	Motif / Précision/Article du Règlement
	(iii) la reconnaissance expresse du notaire selon laquelle la Chambre n'offre aucune garantie quant à la Solution. De plus, le notaire doit s'assurer qu'elle convient à ses besoins.	
10.	Le Prestataire reconnaît que dans le cadre de sa pratique, le notaire traite de renseignements personnels, confidentiels et même sujets au secret professionnel. Conséquemment, le Prestataire s'engage envers le notaire à respecter toutes les exigences légales applicables en matière d'accès à l'information, de protection des renseignements personnels et de respect de la vie privée.	Le Prestataire devra satisfaire aux exigences du projet de loi nº 64 déposé le 12 juin 2020, intitulé *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, notamment en assumant ses responsabilités et en appliquant dans son organisation des mesures de contrôle spécifiques en cette matière.
11.	Le Prestataire s'engage à ne pas utiliser les renseignements personnels, confidentiels et sujets au secret professionnel des notaires ni les métadonnées auxquelles il pourrait avoir accès. Il ne peut non plus les partager, les transférer, les vendre ni plus généralement les communiquer à des tiers sans l'autorisation expresse des personnes concernées ou dans les limites permises par la loi.	
12.	Le Prestataire collaborera avec les représentants autorisés de la Chambre (notamment lors d'enquêtes du syndic).	La Chambre publiera un Guide sur les échanges entre les représentants autorisés de la Chambre et les tiers.

Nº	Bloc 5 : Garanties	Motif / Précision/Article du Règlement
13.	Le Prestataire avise immédiatement le notaire de toute demande d'un tiers autre que la Chambre qui voudrait accéder, consulter ou prendre copie des Documents technologiques d'un notaire.	Protection du secret professionnel.
14.	Le Prestataire souscrit et maintient en vigueur, pendant la durée de l'Entente et pour une durée de 3 ans après la fin de l'Entente, à ses frais et auprès de compagnies d'assurance reconnues, des polices d'assurance générales d'entreprise, responsabilité civile et cyber-risques pour des montants et franchises raisonnables eu égard à l'ensemble de ses activités, à la nature de la Solution et la façon dont elle est exploitée ainsi qu'à sa clientèle.	
15.	Le Prestataire avise la Chambre de son intention de cesser volontairement l'exploitation ou la mise à jour de la Solution au moins 90 jours avant la date effective de cette cessation volontaire.	
16.	Le Prestataire avise la Chambre par écrit de la survenance réelle ou potentielle d'une faillite ou de toute autre procédure le visant en vertu d'une loi d'arrangement entre les créanciers et les débiteurs.	
17.	Le Prestataire avise la Chambre par écrit au plus tard dans les 24 heures de la survenance d'un événement de force majeure ayant pour effet la cessation immédiate de l'exploitation de la Solution.	
18.	Le Prestataire ne pourra céder ses droits et obligations dans l'Entente sans obtenir l'autorisation préalable écrite de la Chambre. La vente ou le transfert des actifs servant à l'exploitation de la Solution ou l'acquisition de contrôle du Prestataire sera réputé constituer une cession des droits du Prestataire dans l'Entente.	

Nº	Bloc 5 : Garanties	Motif / Précision/Article du Règlement
19.	Immédiatement avant la résiliation ou le non-renouvellement de l'Entente : (i) Le Prestataire devra cesser l'attribution de nouvelles SON et ne plus permettre l'utilisation des SON existantes. (i) Le Prestataire devra remettre à la Chambre ou s'assurer que le séquestre l'autorise à remettre à la Chambre tous les Documents technologiques et outils permettant la validation des SON déjà apposées.	
20.	La Chambre ne pourra être tenue responsable de tout dommage résultant du refus d'une Demande d'autorisation ou d'une Révocation d'autorisation, notamment toute perte de revenus de la part du Prestataire.	
21.	La Chambre pourra imposer des pénalités au Prestataire dont les agissements, en contravention du Règlement et de l'Entente, auraient pour effet, par exemple, de compromettre la sécurité de la Solution, de permettre l'utilisation non autorisée d'une SON ou de mettre en péril la pérennité de la validation des SON.	
22.	La conclusion d'une Entente ne confèrera au Prestataire aucun droit dans la propriété intellectuelle de la Chambre et vice versa. Des autorisations expresses seront requises pour l'utilisation de la propriété intellectuelle de l'autre partie.	
23.	Annuellement, à la date d'anniversaire de l'Entente, le Prestataire fournira une déclaration de la direction notamment sur la version de la Solution et les changements dans ses Partenaires, lieux d'hébergement, de sauvegarde et de relève des Documents technologiques.	

Bloc 6 : Généralités

Nº	Bloc 6 : Généralités	Motif / Précision	Commentaire
1.	L'Entente s'interprétera et s'exécutera conformément aux lois applicables au Québec.		
2.	Les différends seront soumis à une procédure d'arbitrage.		
3.	Les avis requis en vertu de l'Entente seront valablement donnés par le biais du Canal de communication ou par courriel sécurisé.		
4.	L'Entente sera à durée indéterminée.		
5.	L'Entente pourra être modifiée en tout temps, par écrit, d'un commun accord entre les Parties.		
6.	L'Entente comportera les engagements habituels relatifs à l'utilisation, au partage et à la destruction des renseignements confidentiels de la Chambre et du Prestataire.		
7.	L'Entente ne confèrera aucun droit exclusif au Prestataire.		

Bloc 7 : Audits

La norme ISO/IEC 27001:2013 stipule ce qui suit: « Il convient de procéder à des revues régulières et indépendantes de l'approche retenue pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) à intervalles définis ou lorsque des changements importants sont intervenus ». L'efficacité d'un SMSI chez le Prestataire dépend de sa mise en œuvre et de son opération selon une démarche d'amélioration continue.

La Chambre réalisera ces revues régulières ou audits selon un programme comportant un audit préalable à la signature de l'Entente, un audit annuel et des audits ponctuels. Ces audits sont aux frais du Prestataire.

La portée d'un audit sera déterminée par la Chambre en fonction du besoin et des motifs qui le sous-tendent, ainsi que de son type (préalable, annuel, ponctuel). Ainsi, un audit pourrait avoir comme portée l'ensemble du SMSI (grille 1 en annexe), des éléments techniques spécifiques à la signature numérique (grille 2 en annexe) et le respect des normes connexes et exigences prévues aux divers Blocs du présent cahier de charges. Il pourrait aussi s'agir d'un audit d'un sous-ensemble de ces éléments, d'un système, d'une solution d'affaires ou d'un service particulier du Prestataire.

La portée de l'audit tiendra aussi compte du fait que le Prestataire possède ou non une certification en vertu des normes ISO/IEC 27001:2013, ISO/IEC 27002:2013 et eIDAS. Le cas échéant, lors de l'audit préalable à la signature de l'Entente, la Chambre exigera minimalement une preuve des certifications ainsi que les deux rapports d'audits les plus récents en vertu de chaque norme, lesquels seront examinés par un auditeur mandaté par la Chambre, aux frais du Prestataire. Ce même auditeur sera chargé de valider la conformité des éléments du présent cahier de charges non couverts par les normes.

Au surplus, le renouvellement des certifications et les rapports d'audit de certification subséquents devront être communiqués sans frais à la Chambre dès qu'ils seront disponibles et ils devront couvrir toute la période sous Entente.

La Chambre mandatera l'auditeur de son choix. Elle pourra également, à sa discrétion, agréer l'auditeur choisi par le Prestataire, s'il présente des garanties suffisantes quant à sa renommée et son indépendance.

Enfin, dans le cas où le Prestataire ne possèderait pas de certification ISO/IEC 27001:2013, ISO/IEC 27002:2013 et eIDAS, ou si la portée de l'audit englobe la conformité d'éléments du présent cahier de charges non couverts par ces normes, l'auditeur fournira un « Rapport d'assurance raisonnable concernant la déclaration sur la conformité » en vertu de la norme NCMC 3530 qui sera adressé à la Chambre.

Nº	Bloc 7: Audits	Motif / Précision	Commentaire
1.	Le Prestataire devra se soumettre au programme d'audits de la Chambre.	Le programme d'audit définit le mode d'opération des audits, le calendrier et les rôles et les responsabilités des parties impliquées.	
2.	Le Prestataire devra désigner un responsable des audits dans son organisation.		
3.	Le rapport d'audit du Prestataire non certifié ISO/IEC 27001:2013, ISO/IEC 27002:2013 et eIDAS ou portant sur des éléments non couverts par ces normes devra être présenté selon la norme NCMC 3530.		
4.	Le Prestataire est tenu de répondre aux écarts constatés lors d'un audit.		

Bloc 8 : Déclarations, garanties et engagements

Dans le cadre d'une demande de conclusion d'Entente en vertu de l'article 6 du *Règlement sur la signature officielle numérique du notaire*	
Par : _____ Nom du fournisseur de signature officielle numérique, soit le « **Prestataire** »	
Par les présentes, le Prestataire garantit à la Chambre des notaires du Québec (la « **Chambre** ») que les éléments qui suivent sont vrais et complets à tous les égards : *(parapher chaque déclaration)*	
1. La personne qui signe ce document est un représentant autorisé du Prestataire.	
2. Il n'a remis aucun cadeau, marque d'hospitalité, gratification ou autre avantage, quelle qu'en soit la nature, sauf ceux d'usage et d'une valeur minime, à un administrateur, dirigeant employé ou membre d'un comité de la Chambre.	
3. L'Office de la protection du consommateur n'a jamais porté plainte à son égard.	
4. Il n'a jamais été inscrit au registre des entreprises non admissibles aux contrats publics, ni ses actionnaires, administrateurs, dirigeants, associés, employés et Partenaires.	
5. Aucun fait ni aucune situation (comme une déclaration de culpabilité ou toute autre action) concernant le Prestataire (incluant ses administrateurs et dirigeants et, dans le cas d'une société privée, ses actionnaires) ne sont susceptibles d'avoir des conséquences négatives importantes pour lui ou pour la Chambre ou ne sont susceptibles d'entacher l'image de la Chambre ou de la profession notariale.	
6. Il n'est pas en faillite, il n'a jamais commis d'actes de faillite au sens de la Loi sur la faillite et l'insolvabilité, il n'est pas insolvable ou visé par une proposition concordataire ou par quelque autre loi d'arrangement entre les créanciers et les débiteurs.	
7. Tous les contrats de travail ou de service entre le Prestataire et les ressources humaines affectées à l'exploitation de la solution de signature officielle numérique contiennent des dispositions sur la protection des renseignements personnels et la confidentialité.	
8. L'ensemble des déclarations, rapports et remises aux autorités fiscales du Prestataire sont à jour.	
9. Si l'une ou l'autre des garanties précédentes devenait inexacte en cours de négociations, préalablement à la conclusion de l'Entente, le Prestataire devra, dans les cinq (5) jours de ce fait, en aviser la Chambre par écrit afin de permettre à cette dernière d'adopter les mesures qu'elle jugera appropriées.	
10. Le Prestataire accepte que le fait pour une déclaration contenue aux présentes de devenir fausse ou incomplète puisse entraîner la résiliation de l'Entente.	
11. Le Prestataire a lu et compris la portée du présent document.	
12. Le Prestataire reconnaît que si les déclarations contenues aux présentes ne sont pas vraies ou complètes à tous les égards, le Prestataire ne pourra pas conclure d'Entente avec la Chambre pour la fourniture d'une signature officielle numérique aux notaires.	
13. Le Prestataire reconnaît et accepte que les déclarations contenues aux présentes puissent être utilisées à des fins extrajudiciaires, judiciaires, de médiation ou d'arbitrage.	

Si l'une des déclarations précédentes ne peut être paraphée, veuillez en expliquer la raison dans une annexe, joindre tout document afférent et cocher cette case :	
Et le Prestataire a signé :	
Signature du Prestataire	Date
Nom du signataire autorisé du Prestataire en lettres moulées et titre	

Annexe: Grilles d'exigences

Grille #1 Organisation de la sécurité de l'information

Les notaires ont des objectifs et des obligations qui sont élevés en ce qui concerne la sécurité de l'information. L'atteinte de ceux-ci est possible avec des mesures de sécurité organisationnelles et techniques (méthodes, pratiques, politiques, processus, objectifs, moyens technologiques) chez le Prestataire.

La grille 1 ci-après présente les attentes de la Chambre envers le Prestataire en regard de son SMSI. Elle présente les clauses et les articles des normes ISO/IEC 27001:2013 et ISO/IEC 27002:2013 auxquelles le Prestataire doit se conformer dans le contexte qui est décrit dans ce cahier de charges.

Nº	Grille 1 SMSI : Clauses, Sections et Contrôles	Motif / Précision
Les lignes 1 à 4 de cette grille présentent les clauses de la norme ISO27001:2013 qui doivent être effectives dans le SMSI du Prestataire.		
1	L'implémentation de la sécurité de l'information chez le Prestataire s'appuie sur les normes ISO127001:2013 et ISO27002:2013.	Les clauses, sections et mesures de contrôles des normes qui sont choisies par le Prestataire pour être implémentées sont listées dans une Déclaration d'applicabilité. Un audit utilise cette déclaration comme intrant.
2	L'implémentation de la sécurité de l'information est documentée et à jour.	
3	Le Prestataire a un processus de gestion des risques qui est effectif.	Ce processus du Prestataire devra intégrer la Chambre comme une partie prenante dans l'identification et l'évaluation des risques.
4	Le Prestataire a un processus d'amélioration continue de sa sécurité de l'information.	
5	*A.5 Politiques de SI* *A.5.1 Engagement du management* *A.5.1.1 Politique pour la SI* *A.5.1.2 Revue de la politique de sécurité*	L'équipe de direction du Prestataire définit et fait la gouvernance de la sécurité de l'information.

Nº	Grille 1 SMSI : Clauses, Sections et Contrôles	Motif / Précision
6	*A.6 Organisation de la sécurité de l'information / SI* *A.6.1 Organisation interne* *A.6.1.1 Rôles et responsabilités de la SI* *A.6.1.2 Séparation des tâches* *A.6.1.3 Contact avec les autorités* *A.6.1.4 Contact avec les groupes d'intérêt* *A.6.1.5 SI dans la gestion de projet*	Les rôles et les responsabilités en regard de la sécurité de l'information sont clairement définis dans l'organisation du Prestataire.
7	*A.7 Sécurité des ressources humaines* *A.7.1 Avant l'engagement* *A.7.1.1 Vérification des antécédents* *A.7.1.2 Termes et conditions d'emploi* *A.7.2 Durant l'emploi* *A.7.2.1 Responsabilité de la gestion* *A.7.2.2 Sensibilité, éducation et formation sur les SI* *A.7.2.3 Mesures disciplinaires* *A.7.3 Fin ou changement d'emploi* *A.7.3.1 Fin ou changement des responsabilités*	La gestion des ressources humaines chez le Prestataire prend en compte la sécurité de l'information, notamment par une vérification des antécédents judiciaires, de la formation et de la sensibilisation de son personnel à la sécurité de l'information.
8	*A.8 Gestion des actifs* *A.8.1 Responsabilité envers les actifs* *A.8.2 Information classifiée* *A.8.2.1 Classification de l'information* *A.8.3 Manipulation des actifs*	La gestion des actifs informationnels du Prestataire est documentée et effective afin d'assurer sa disponibilité, son intégrité et sa confidentialité.
9	*A.9 Contrôle d'accès* *A.9.1 Exigences d'affaires pour le contrôle d'accès* *A.9.1.1 Politique (ou règles) pour le contrôle d'accès* *A.9.1.2 Contrôle d'accès au réseau et aux services réseaux*	Le Prestataire a mis en œuvre les mesures de contrôle adéquates pour assurer un contrôle d'accès physique et logique de ses actifs.

Nº	Grille 1 SMSI : Clauses, Sections et Contrôles	Motif / Précision
	A.9.2 Gestion des accès des utilisateurs *A.9.2.1 Processus d'enregistrement et dé-enregistrement des utilisateurs* *A.9.2.2 Gestion du cycle de vie des utilisateurs* *A.9.2.3 Gestion des utilisateurs avec des accès privilégiés* *A.9.2.4 Gestion des informations d'authentification des utilisateurs* *A.9.2.5 Revue des droits d'accès* *A.9.2.6 Retrait et modification des droits d'accès* *A.9.3 Responsabilités des utilisateurs* *A.9.3.1 Règle d'utilisation des informations d'authentification* *A.9.4 Contrôle d'accès aux systèmes et aux applications* *A.9.4.1 Contrôle d'accès aux informations* *A.9.4.2 Procédures sécuritaires d'authentification* *A.9.4.3 Gestion des mots de passe* *A.9.4.4 Contrôle de l'utilisation des programmes privilégiés* *A.9.4.5 Contrôle d'accès aux codes sources*	
10	*A.10 Cryptographie*	Cette clause est détaillée dans la grille 2 spécifique à l'infrastructure à clés publiques.
11	*A.11 Sécurité physique et environnementale*	Le Prestataire ainsi que ses Partenaires ont déployé les mesures de contrôle physique adéquates selon le contexte, le lien et la nature des moyens utilisés.
12	*A.12 Gestion des opérations* *A.12.1 Responsabilités et processus opérationnels* *A.12.1.1 Documentation des processus* *A.12.1.2 Gestion du changement* *A.12.1.3 Gestion de la capacité management* *A.12.1.4 Séparation des environnements de production, développement et essai* *A.12.2 Protection contre les logiciels malveillants* *A.12.2.1 Mesure de contrôle contre les logiciels malveillants*	Le Prestataire doit documenter, mettre en œuvre et assigner les ressources nécessaires pour ses opérations et le maintien des niveaux de services dans une démarche d'amélioration continue.

Nº	Grille 1 SMSI : Clauses, Sections et Contrôles	Motif / Précision
	A.12.3 Copie de sécurité *A.12.3.1 Copie des informations* *A.12.4 Journaux et surveillance* *A.12.4.1 Journalisation des événements* *A.12.4.2 Protection des journaux* *A.12.4.3 Administrateur et les journaux des opérateurs* *A.12.4.4 Horloge synchronisée* *A.12.5 Contrôle des logiciels* *A.12.5.1 Installation des logiciels autorisés (whitelisting)* *A.12.6 Gestion des vulnérabilités techniques* *A.12.6.1 Gestion des vulnérabilités techniques* *A.12.6.2 Contrôle des logiciels installés par l'utilisateur* *A.12.7 Considérations pour les audits des systèmes* *A.12.7.1 Planification des audits des systèmes*	
13	*A.13 Sécurité des communications* *A.13.1 Gestion de la sécurité du réseau* *A.13.1.1 Mesures de contrôles réseautiques* *A.13.1.2 Sécurité du réseau* *A.13.1.3 Ségrégation dans le réseau* *A.13.2 Transfert des informations*	La Prestataire déploie les mesures de contrôle adéquates pour protéger l'information lors du transport, en transit et au repos.
14	*A. 14 Acquisition, développement et maintenance des systèmes d'information* *A.14.1 Exigences de sécurité pour les systèmes d'information* *A.14.2 Sécurité dans le développement et le support* *A.14.3 Données d'essais* *A.14.3.1 Protection des données d'essais*	Le développement et l'entretien des logiciels du Prestataire sont réalisés avec une méthode de développement sécuritaire logicielle**.** En aucun cas, les données de production ne sont utilisées pour le développement.

Nº	Grille 1 SMSI : Clauses, Sections et Contrôles	Motif / Précision
15	*A.15 Relations avec les fournisseurs*	Si le Prestataire utilise les services d'un Partenaire ou des services en mode infonuagique publics, il doit en informer la Chambre dans son offre de services. Ces Partenaires doivent offrir une sécurité de l'information qui est égale ou supérieure à celle exigée par la Chambre.
16	*A.16 Gestion des incidents de sécurité* *A.16.1 Gestion des incidents de sécurité* *A.16.1.1 Établissement des processus et des responsabilités* *A.16.1.2 Déclaration des incidents de sécurité* *A.16.1.3 Déclaration des vulnérabilités* *A.16.1.4 Évaluation et classement des incidents de sécurité* *A.16.1.5 Réponse aux incidents de sécurité* *A.16.1.6 Amélioration continue et correction à la suite d'incidents de sécurité* *A.16.1.7 Collecte de la preuve*	Le processus de gestion des incidents du Prestataire est arrimé avec celui de la Chambre en conformité avec les exigences de l'Entente et du Bloc 3 : des modalités administratives.
17	*A.17 Continuité de service et sécurité de l'information* *A.17.1 Continuité de service* *A.17.1.1 Planification de la continuité de service* *A.17.1.2 Implémentation de la continuité de service* *A.17.1.3 Vérification, revue et évaluation de la continuité de service* *A.17.2 Infrastructure redondante* *A.17.2.1 Disponibilité des infrastructures de continuité de service*	Le Prestataire doit partager et démontrer comment il prend en charge la continuité de service. Il doit présenter sa stratégie, la mise en œuvre et les essais qu'il réalise.
18	*A.18 Conformité* *A.18.1 Conformité au cadre légal et au cadre contractuel*	Le Prestataire devra satisfaire aux exigences du projet de loi nº 64 déposé le 12 juin 2020, intitulé *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, notamment en assumant ses

Nº	Grille 1 SMSI : Clauses, Sections et Contrôles	Motif / Précision
	A.18.1.1 Identification des clauses légales et contractuelles applicables *A.18.1.2 Propriété intellectuelle* *A.18.1.3 Protection des renseignements* *A.18.1.4 Protection des renseignements personnels et de la vie privée* *A.18.1.5 Conformité légale de l'utilisation de la cryptographie* *A.18.2 Audit de l'implantation de la sécurité de l'information* *A.18.2.1 Indépendance de l'audit* *A.18.2.2 Conformité aux politiques et aux normes* *A.18.2.3 Audit technique*	responsabilités et en appliquant dans son organisation des mesures de contrôle spécifiques en cette matière. La question des audits est abordée dans le Bloc 7.

Grille #2 Éléments techniques spécifiques à la signature numérique

La grille 2 ci-après présente les attentes de la Chambre envers le Prestataire en regard de son infrastructure à clés publiques (ICP).

Nº	Grille 2 ICP : Clauses, Sections et Contrôles	Motif / Précision
1	La solution proposée par le Prestataire doit être fonctionnelle tout en cohabitant avec les logiciels et les certificats des solutions actuellement en opération chez les notaires comme mentionné dans la section "Mise en garde" de ce cahier de charges.	
2	Les transactions monétaires en ligne (solution de paiement) qui sont offertes par la solution du Prestataire doivent être traitées par un système certifié selon la norme PCI.	
3	Les normes relatives à l'opération de l'ICP qui sont retenues par le Prestataire doivent être conformes ou être compatibles au cadre normatif eIDAS (Electronic IDentification Authentication and trust Services).	Malgré que ce soit un cadre normatif européen, eIDAS constitue une référence reconnue mondialement. La conformité attendue est détaillée dans les lignes suivantes et dans le reste du cahier de charges.
4	Le niveau de confiance du service du Prestataire et des processus de gestion des certificats et d'inscription des utilisateurs doit permettre d'établir un niveau de confiance moyen-élevé de la signature numérique au minimum. Toutefois, un niveau de confiance substantiel selon le cadre normatif eiDAS (qualified digital certificates) est nettement favorisé.	Ceci détermine des mesures d'intégrité, d'identité et de traçabilité élevées : • horodatage; • clés et certificat sur un dispositif protégé; • processus d'identification et de validation.
5	La solution proposée par le Prestataire doit permettre de signer des documents produits selon les normes : • PDF/A • PDF/A2 • ISO 19005 (signer de façon pérenne des documents)	
6	Le Prestataire doit produire et rendre accessible sa politique d'opération et les exigences de son ICP en conformité avec les clauses pertinentes des normes suivantes : • ETSI EN 319 401 (Politique) • ETSI EN 319 411-1 (Exigences)	

Nº	Grille 2 ICP : Clauses, Sections et Contrôles	Motif / Précision
	• ETSI EN 319 413-1 (Exigences pour le légal) Le document de politique d'opération et d'exigences doit couvrir ces éléments : 1. Structure organisationnelle a. Plan de sécurité b. Plan de communication c. Plan de gestion des risques d. Plan de continuité des activités e. Plan de gestion des incidents f. Plan d'audit g. Plan de formation h. Plan d'application légale i. Plan de contrôle d'accès 2. Politiques a. Politique de certification b. Politique d'archivage c. Approbation des politiques internes 3. Registres de conformité légale a. Énoncé des pratiques de certification (Certification Practice Statement : CPS) b. Responsabilités de publication et de dépôt c. Identification et authentification d. Exigences opérationnelles du cycle de vie du certificat e. Contrôle des installations, de la gestion et des opérations f. Contrôles techniques de sécurité 4. Mise en œuvre a. Service d'enregistrement	

Nº	Grille 2 ICP : Clauses, Sections et Contrôles	Motif / Précision
	b. Service de génération de certificats c. Service de mise à disposition des appareils en question d. Service de diffusion e. Service de révocation f. Motifs de révocation d'un certificat d'abonné g. Motifs de révocation d'un certificat d'AC subordonné 5. Profils a. Profil de certificat b. Profil CRL c. Profil OCSP 6. Service de révocation et de validation a. CRL b. OCSP	
7	La solution proposée par le Prestataire doit permettre la récupération des clés de chiffrement (le cas échéant) si elles sont perdues ou détruites : ETSI EN 319 411-1: 6.3.12 Key escrow and recovery	