

CONDITIONS PARTICULIÈRES D'UTILISATION DES PRODUITS OFFERTS PAR SOLUTIONS NOTARIUS – CERTIFIO^{MD} (ci-après les « Conditions particulières »)

Entre **SOLUTIONS NOTARIUS INC.**, une entreprise Portage Cybertech, ayant un établissement au 465, rue McGill, bureau 300, Montréal, Québec, Canada, H2Y 2H1 (« **Notarius** ») et vous (ci-après « **vous** », l'« **Acheteur** », le « **Détenteur** », l'« **Organisation** », l'« **Entité** » ou le « **Regroupement de professionnels** » selon le cas applicable) (individuellement désigné une « **Partie** » et conjointement désignés les « **Parties** »).

Depuis 1998, l'autorité de certification (AC) Notarius, basée sur une infrastructure à clés publiques (ICP), est reconnue et utilisée avec confiance par divers organismes gouvernementaux. En 2007, Notarius est devenue la première autorité de certification en Amérique du Nord à être certifiée ISO 27001 (gestion de la sécurité de l'information). Pionniers en matière de confiance numérique, Notarius agit à titre de membre actif du Conseil d'identification et d'authentification numériques du Canada (CCIAN), de la Fédération des Tiers de Confiance du Numérique (FNTC) et de la PDF Association. Notarius est la seule entreprise canadienne à émettre des certificats de signatures numériques (ci-après « Signatures numériques ») de confiance reconnues par Adobe (Adobe Approved Trust List – AATL) et Microsoft (Microsoft Trusted Root Certificate Program).

À titre de prestataire de service de certificat et de répertoires (« PSC/R »), Notarius a eu depuis de longues années pour mission d'offrir des solutions de Signatures numériques (certificat de signature numérique sur epf. ou jeton cryptographique) assurant la fiabilité à long terme des documents.

Se tenant à l'avant-garde de la technologie, à l'écoute des besoins de ses parties prenantes et compte tenu de l'évolution des technologies, de la place toujours plus importante de l'infonuagique (« Cloud ») et des équipements mobiles notamment, Notarius se devait de bonifier son offre de Produits. À ce titre, la nouvelle solution de Signature numérique Cloud de Notarius, « *CertifiO Cloud* » permet désormais aux Détenteurs de signer numériquement des documents sans avoir besoin de préalablement installer localement sur leurs postes de travail des éléments du certificat de signature (par exemple la clé privée).

Notarius propose également à ses clients une solution de sécurisation des documents par code à barre, le cachet électronique visible (CEV – « *CertifiO Code* »), qui comprend les données clés signées électroniquement permettant de détecter toute altération et de confirmer l'authenticité et la légitimité de l'émetteur.

Notarius vous accorde, en contrepartie du paiement des sommes requises, une licence d'utilisation non exclusive, ne pouvant pas être transférée ou cédée à un tiers entièrement ou en partie, de CertifiO selon les modalités ci-dessous décrites.

En souscrivant et en utilisant CertifiO, vous consentez et acceptez les présentes Conditions particulières.

1. DISPOSITIONS GÉNÉRALES

Sujet à changements parfois importants

LES PRÉSENTES CONDITIONS PARTICULIÈRES COMPLÈTENT LES [CONDITIONS GÉNÉRALES](#) ET ENSEMBLE, ELLES RÉGISSENT VOTRE UTILISATION DE CERTIFIO. LES CONDITIONS GÉNÉRALES SONT RÉPUTÉES FAIRE PARTIE INTÉGRANTE DES PRÉSENTES.

- 1.1. Les Produits de la gamme CertifiO permettent aux Détenteurs de signer numériquement leurs documents. Tous les produits CertifiO incluent les licences et certificats de signature nécessaires pour signer vos documents électroniques afin de préserver l'origine, l'intégrité et l'authenticité du document signé.
- 1.2. Les Produits de la gamme CertifiO vous permettent d'obtenir et d'utiliser un certificat de Signature numérique avec vérification d'identité ou d'entité et certification du statut professionnel ou du lien d'emploi du Détenteur lorsqu'applicable.
- 1.3. Les documents signés avec un Produit de la gamme CertifiO vous permettent de certifier l'identité ainsi que le statut professionnel ou l'affiliation à une Organisation du signataire.
- 1.4. Pour être habilité à souscrire à certains Produits de la gamme CertifiO, votre employeur doit préalablement avoir ouvert un compte corporatif chez Notarius. Également, seul votre courriel professionnel nominatif associé à cet employeur devra être utilisé lors de votre adhésion au Produit.

2. DÉFINITIONS

Les termes non définis aux présentes Conditions particulières ont le sens qui leur est attribué dans les Conditions générales ou dans les Politiques de certification ou les Déclarations des pratiques de certification de Notarius.

- 2.1. « **AATL ou Adobe Approved Trust List** » : Tel que défini par Adobe, programme (référant à une liste de prestataires autorisés) permettant à des millions de personnes à travers le monde de signer numériquement les documents en utilisant les identités numériques les plus fiables. Les Autorités de Certification (AC) et les Tiers de Confiance figurant sur la liste AATL émettent des certificats numériques permettant l'horodatage certifié et l'apposition de signatures fondées sur les identités numériques fiables en conformité avec les plus hautes exigences légales et réglementaires du monde entier. AATL est une fonctionnalité d'Adobe offerte sur certaines signatures numériques Notarius, mais pas toutes, résultant en la reconnaissance par défaut des signatures Notarius dans tous les logiciels Adobe.
- 2.2. « **Agent vérificateur d'identité (AVI)** » : Employé autorisé du PSC/R pour procéder aux vérifications d'identité des personnes physiques Acheteurs de certificats selon les spécifications détaillées dans la Politique de certification de Notarius (notamment la complétion d'un formulaire web spécifique au produit acheté, la prise d'un rendez-vous aux fins de présentation des pièces justificatives requises de l'identité). Dans certains cas et sous certaines conditions, des organisations peuvent bénéficier d'une autorisation spécifique

Sujet à changements parfois importants

pour procéder elles-mêmes aux vérifications d'identité - Ici un AVI et un agent vérification d'affiliation (AVA) devront être expressément nommés. Par exemple, pour les professionnels notaires, la VI doit obligatoirement être faite par un notaire conformément à l'art 3 du Règlement sur la signature officielle numérique du notaire, N-3, r. 13.1.

- 2.3. « **Application client** » : L'application ou le logiciel utilisé par le Détenteur, installé sur un poste ou accessible en ligne, qui permet par exemple d'activer ou de récupérer ses certificats, de modifier son mot de passe, d'effectuer certaines opérations de configuration ou de réaliser des transactions au moyen de ses certificats.
- 2.4. « **Autorité de certification (AC)** » : Entité responsable des certificats signés en son nom ainsi que de l'ensemble de l'ICP.
- 2.5. « **Bi clé ou Paire de clés** » : 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.
- 2.6. « **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 CP de Notarius est le CEV Otentik, dont la gouvernance est dictée par l'AIGCEV.
- 2.7. « **CertifiO Code** » : Certificat de signature numérique signant le CEV afin d'en assurer l'intégrité et l'authenticité. Délivré pour un ou des cas d'usage spécifiques tels qu'autorisés par l'AIGCEV. Est émis à un organisme généralement responsable de l'émission des documents sur lesquels le CEV sera apposé. Utilisé en conjonction avec les solutions ConsignO^{MD} Serveur et les solutions VerifiO^{MD}, vous pourrez ainsi créer, apposer et valider un CEV sur un document imprimé afin d'en assurer l'intégrité et l'authenticité.
- 2.8. « **CertifiO pour Département** » : Certificat de signature numérique certifiant le nom du département d'une Organisation et associant le document signé avec ce certificat au département de ladite Organisation. La signature est réalisée par un employé au nom de l'Organisation, pour un maximum de 2 000 signatures annuellement. Les informations quant à l'identité du signataire ne sont pas incluses dans ce certificat.
- 2.9. « **CertifiO pour Employés** » : Certificat de Signature numérique pour les employés certifiant l'identité du Détenteur et son lien d'emploi avec une Organisation cliente de Notarius. Ce certificat de signature numérique est à l'usage exclusif du Détenteur identifié au certificat.

Sujet à changements parfois importants

- 2.10. « **CertifiO pour Évaluation** » : Certificat de signature numérique pour évaluation uniquement; ne peut être utilisé dans un objectif différent. 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.
- 2.11. « **CertifiO pour Organisation** »: Certifie l'organisation d'où origine le document. Ce type de certificat de signature numérique est généralement intégré dans un processus automatisé sur un serveur pour de grands volumes de documents signés annuellement. Ce type d'abonnement est basé sur le volume annuel de documents signés et nécessite un lot de licences correspondant. Les certificats de signatures numériques pour Organisations sont toujours AATL.
- 2.12. « **CertifiO pour professionnels** »: Certificat de signature numérique, certifiant l'identité et le statut professionnel du signataire. Ce certificat de signature numérique est pour l'usage exclusif du professionnel nommé dans le certificat. Le numéro de membre ainsi que le nom légal de l'Ordre professionnel est indiqué dans le Certificat. Ce type de Produit requiert la signature d'une entente formelle entre Notarius et l'Ordre ou le Regroupement de professionnels.
- 2.13. « **Clé privée** » : La clé d'une paire de clés qui est gardée secrète par le détenteur de la paire de clés et qui est utilisée pour créer des Signatures numériques ou pour déchiffrer des documents qui ont été chiffrés avec la clé publique correspondante.
- 2.14. « **Clé publique** » : La clé d'une paire de clés qui peut être divulguée publiquement par le détenteur de la clé privée correspondante et qui est utilisée par une partie utilisatrice pour vérifier les signatures numériques créées avec la clé privée correspondante du détenteur ou pour chiffrer un document par exemple afin qu'il ne puisse être déchiffré qu'avec la clé privée correspondante du détenteur.
- 2.15. « **Compromission de la clé** » : On parle de compromission d'une clé privée lorsque sa valeur a été divulguée à une personne non autorisée, si une personne non autorisée y a eu accès ou s'il existe une technique pratique par laquelle une personne non autorisée puisse en découvrir la valeur.
- 2.16. « **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.

Sujet à changements parfois importants

- 2.17. « **HSM Hébergé** » : Le certificat de signature numérique, partie de la solution CertifiO pour organisations (AATL), est hébergé sur HSM certifié par Notarius pouvant être interrogé à distance pour signer des données en utilisant le certificat de l'Entité (i.e. organisation). Ce type d'abonnement est basé sur le volume annuel de documents signés et nécessite un Lot de signatures correspondant.
- 2.18. « **Infrastructure à clés publiques (ICP)** » : Ensemble de composants physiques, de fonctions et procédures, de logiciels et de ressources humaines dédiés à la gestion des clés et certificats émis par l'AC.
- 2.19. « **Logiciel de Signature numérique** » : Logiciel utilisé pour lier de manière cryptographique un certificat de signature numérique à un document. Les utilisateurs sont libres d'utiliser n'importe quel Logiciel de signature numérique conforme aux normes et pouvant accéder et utiliser des certificats de signature numérique.
- 2.19.1. Notarius fournit aux Détenteurs de **Signature numérique desktop**, un Logiciel de signature numérique, commercialisé sous le nom de *ConsignO Desktop*, vous permettant d'effectuer les opérations avancées suivantes:
- a) Définir des modèles de zones de Signature numérique
 - b) Signer numériquement, y compris la Signature numérique en lot;
 - c) Convertir et vérifier de la conformité à la norme PDF/A.
- 2.19.2. Notarius fournit aux Détenteurs de **Signature numérique Cloud**, une Application web, commercialisée sous le nom de *ConsignO Cloud Solo*, vous permettant de signer numériquement au moyen de votre signature numérique CertifiO Cloud individuelle afin de produire un document à haut degré de conformité. L'accès à cette application vous est alloué via une authentification à votre compte Notarius (« Mon Compte ») suite à l'adhésion au produit CertifiO Cloud.
- 2.20. « **Mon Compte** » : Le compte Notarius est un compte en ligne sécurisé (nom d'utilisateur / 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 de la Signature numérique du Client.
- 2.21. « **PDF/A** » : La norme ISO 19005 garantissant que les documents électroniques peuvent être ouverts et lus sur de longues périodes de temps.
- 2.22. « **Politiques de certification (CP)** » : Ensemble de règles, identifiés par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations. Ces documents officiels sont disponibles sur le site Web de Notarius ici :

Sujet à changements parfois importants

<https://www.notarius.com/fr/politiques-de-certification-et-declarations-des-pratiques>.

- 2.23. « **Prestataire de services de certificat 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.
- 2.24. « **Révocation** » : Retrait d'un certificat effectué de plein droit par le PSC/R ou à la demande d'une personne autorisée.

3. RESPONSABILITÉS ET OBLIGATIONS DE L'UTILISATEUR FINAL, DU DÉTENTEUR, DE L'ACHETEUR, DE L'ENTITÉ, DE L'ORGANISATION, DU REGROUPEMENT DE PROFESSIONNELS OU DE SES AVA AUTORISÉS

Les Produits de la gamme CertifiO vous permettent d'apposer une signature numérique certifiant votre identité ou celui du département ou de l'organisation signataire, ainsi que votre statut professionnel ou votre lien d'emploi, lorsqu'applicable.

À ce titre, vous consentez, vous acceptez, vous reconnaissez et vous vous engagez à:

- 3.1. Utiliser les Produits de Notarius conformément aux obligations des présentes incluant les Conditions générales et celles décrites dans les Politiques de Certifications et les Déclarations des Pratiques de Certification adoptées par Notarius.
- 3.2. Ne fournir à Notarius que des informations et/ou Renseignements personnels véridiques, exacts, à jour et complets. Procéder immédiatement aux mises à jour requises de vos informations et/ou Renseignements personnels (notamment votre courriel ou votre numéro de téléphone) lorsqu'applicables.
- 3.3. Fournir une adresse courriel nominative et liée à votre employeur lors de votre Abonnement au Produit CertifiO pour Employés (Cloud comme Desktop).
- 3.4. Fournir, pour toutes demandes d'Abonnement au produit CertifiO pour Organisation, Département, CEV ou pour toute ouverture de compte d'entreprise, le nom légal officiel et actif de votre Organisation tel qu'il est enregistré auprès des autorités compétentes (par exemple registraire des entreprises). Si votre organisation est enregistrée dans une province où l'accès au registre est payant ou encore à l'étranger, vous vous engagez à joindre à votre demande une copie officielle récente du registre qui prouvera de cette existence légale dans l'une des deux (2) langues officielles du Canada (en français ou en anglais).
- 3.5. Réserver votre vérification d'identité devant un AVI autorisé qui effectuera les vérifications nécessaires et recueillera certains de vos Renseignements personnels, lesquels seront traités conformément à la Politique de confidentialité et les Politiques de certification de Notarius.
- 3.6. Présenter des pièces d'identité originales, valides et émises par une autorité gouvernementale reconnue lors de votre vérification d'identité avec l'AVI autorisé.

Sujet à changements parfois importants

- 3.7. Autoriser Notarius, à utiliser vos Renseignements personnels pour les fins de votre identification dans le cadre de la fourniture des Produits. Pour les détails, concernant la Vérification d'Identité, voir les Déclarations des pratiques de Certification de Notarius correspondantes au Produit acheté.
- 3.8. Être entièrement responsable de la préservation de la confidentialité de votre mot de passe, de vos codes d'identification ou de vos questions et réponses de sécurité le cas échéant servant à vous identifier et vous permettant d'accéder à l'espace Mon Compte. La perte du mot de passe peut empêcher l'accès aux Produits.
- 3.9. Reconnaître que l'utilisation de votre Signature numérique est un DROIT PERSONNEL et qu'il est STRICTEMENT INTERDIT de confier ou encore de divulguer à quiconque les informations permettant de l'utiliser. Une violation de cette obligation pourrait non seulement entraîner la révocation de votre certificat de Signature numérique sans autre avis ou délai, mais également être notifiée sans délais et sans autre avis à votre Ordre ou Association professionnelle pour les Détenteurs de Signature numérique pour professionnels.
- 3.10. Reconnaître que vos Renseignements personnels (informations de contact notamment) peuvent être utilisés par des tiers qui veulent présenter à Notarius la preuve de la compromission de votre clé privée (par exemple en signant une demande de révocation du certificat à l'aide de ladite clé privée), afin que votre certificat de signature numérique correspondant puisse être révoqué.
- 3.11. Valider que l'aspect de signature appliqué à votre document est conforme avec les requis de votre Ordre ou Association professionnelle. Vous vous engagez également à signer avec l'aspect de signature associé à la signature numérique sélectionnée dans les cas par exemple où vous êtes détenteurs de plusieurs Signatures numériques (Desktop comme Cloud).
- 3.12. Faire en sorte que, dans les cas de l'achat de certificat annuel de HSM hébergé, par votre propre Client, que celui-ci :
 - 3.12.1. Accepte également de se conformer aux Conditions d'utilisation des Produits et de la Politique de certification dédiée de Notarius.
 - 3.12.2. Joigne à sa demande une copie récente, à jour et valide du registre qui prouvera son existence légale.
 - 3.12.3. Fournisse des informations et/ou Renseignements personnels véridiques, exacts et complets et vous avise de toute modification des informations contenus dans le certificat.
 - 3.12.4. Est responsable de l'utilisation inappropriée de ses clés par ses employé, administrateurs ou autres.
 - 3.12.5. Reconnaisse et accepte que (i) vous seul êtes responsable de la protection des informations de connexion de l'organisation, y compris, mais sans s'y limiter, son nom d'utilisateur/mot de passe ou sa clé de signature/secret API, selon le cas; (ii) également et si applicable, reconnaît et accepte que vous avez la possibilité de supprimer les projets de signature de son compte ou de transmettre ou envoyer les Projets de Signature à un mauvais destinataire; (iii) également et si applicable, reconnaît et accepte que vous puissiez avoir accès au certificat et clé de signature et, en ce sens, que vous seul seriez

Sujet à changements parfois importants

responsable de l'utilisation inappropriée de ces clés; (iv) dégage de toute responsabilité Notarius quant à l'utilisation erronée de son certificat par vous.

- 3.13. Respecter et à faire respecter par les Utilisateurs Finaux les licences des concédants de licence de Notarius contenues dans la suite CertifiO.
- 3.14. Veiller à la configuration adéquate, de même que l'obtention et le paiement des équipements et des services de tiers nécessaires à votre accès ou à votre utilisation des Produits, notamment, mais sans s'y limiter, tout accès Internet.
- 3.15. Instaurer des politiques et autres pratiques administratives internes pour notamment prévenir les accès, utilisations, modifications ou divulgations non autorisés des Produits par des parties non autorisées via les équipements sous votre contrôle.
- 3.16. Aviser immédiatement Notarius en cas de soupçon de Compromission de la clé ou de perte de votre certificat de Signature numérique.
- 3.17. Former vos Utilisateurs Finaux, lorsqu'applicable et veiller à ce qu'ils utilisent les Produits conformément aux directives données par Notarius de temps à autre.
- 3.18. Fournir des renseignements justes, précis, exacts et complets et informer Notarius de tout changement dans les meilleurs délais, notamment tout changement au sein de votre organisation ou toute révocation temporaire ou permanente d'un Détenteur, ou d'un Utilisateur Final autorisés à agir en votre nom et à utiliser les Produits.
- 3.19. Vérifier la validité ou la révocation de votre Signature numérique en utilisant les informations actuelles sur l'état de révocation de votre certificat ou le statut de vos abonnements identifiés dans « Mon compte ». De plus, NE PLUS UTILISER le support ayant contenu la Signature Numérique révoquée.
- 3.20. Approuver ou rejeter, les demandes d'abonnement, lorsque requis. L'approbation inclut la confirmation du lien d'emploi lorsqu'applicable.
- 3.21. Révoquer les certificats lorsque le lien d'emploi est rompu ou que le Détenteur n'est plus un membre actif de l'Ordre ou Association professionnelle.

4. RESPONSABILITÉS ET OBLIGATIONS DE NOTARIUS

- 4.1. Fourniture des Produits. Sous réserve du paiement de tous les frais applicables et du respect de toutes les Conditions d'utilisation, incluant les Conditions particulières et générales, Notarius s'engage à fournir les Produits à l'Acheteur et ces Produits seront rendus substantiellement conformément à leurs Spécifications. L'Acheteur accepte par ailleurs que les Produits puissent être fournis, en tout ou en partie, par un tiers.
- 4.2. Autorité de certification. Notarius agit comme Autorité de Certification ou

Sujet à changements parfois importants

Prestataire de Service. À ce titre, Notarius est responsable d'émettre les certificats de Signatures Numériques et de faire les vérifications préalables requises à leur émission.

- 4.3. Vérification de l'identité. Afin d'émettre une Signature Numérique, Notarius doit vérifier (sauf pour les notaires voir 2.2) l'identité du Détenteur et/ou de l'Utilisateur Final, selon le cas applicable. Par conséquent, certains Renseignements personnels devront être communiqués à Notarius, le tout selon les indications transmises par le Détenteur et/ou à l'Utilisateur Final pour ce faire. Vous autorisez donc Notarius, dans le cadre de la fourniture du Produit, à utiliser vos Renseignements personnels. Également vous autorisez Notarius à conserver les preuves de votre vérification d'identité un minimum de 10 ans à compter de la date anniversaire de l'annulation de votre abonnement.
- 4.4. Logs d'activité des Signatures numérique. Les journaux d'évènements liés à votre Signature numérique sont conservés un minimum de 10 ans à compter de la date anniversaire de l'expiration ou de la révocation de votre certificat.
- 4.5. Si des paires de clés sont générées par Notarius pour le compte de l'Acheteur et offertes sous forme d'options PKCS#12, Notarius s'efforcera d'utiliser des systèmes dignes de confiance pour générer ces paires de clés notamment une plateforme reconnue comme étant adaptée à cet effet, s'assurera que les clés privées sont cryptées si elles sont transportées vers le Détenteur, utilisera une longueur de clé et un algorithme qui sont reconnus comme étant adaptés à l'objectif de la signature numérique et, pour les CEV ne signera pas les paires de clés inférieures à 2048 bits notamment.
- 4.6. Escalade des bris de sécurité à votre Ordre ou Association professionnelle. Dans le respect de 3.9, Notarius pourrait devoir notifier l'Ordre ou Association professionnelle du Détenteur en cas de compromission soupçonnée ou avérée de son certificat de Signature numérique.

5. DISPOSITIONS SPÉCIFIQUES À CERTIFIO POUR PROFESSIONNELS

- 5.1. Modifications des prix par un Regroupement de Professionnels: Les Regroupements de Professionnels qui facturent leurs membres respectifs pour les services relatifs au Produit CertifiO pour professionnels se réservent également le droit de changer leurs propres tarifs à tout moment. Les tarifs ainsi modifiés s'appliqueront immédiatement et devront être communiqués par les Regroupements de Professionnels par l'envoi d'un avis écrit à leurs membres à cet effet. Le Client qui n'accepte pas cette augmentation pourra révoquer sa Signature numérique CertifiO pour professionnels via « Mon Compte ».

6. FIN DE VIE DE L'AC ET ENTIÈREMENT

- 6.1. Si des LCR sont fournies et que Notarius 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.

Sujet à changements parfois importants

- 6.2. 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.

- 6.3. 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.
- 6.4. 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.
- 6.5. 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.
- 6.6. Notarius n'émettra pas de dernière LCR avant que tous les certificats visés par cette LCR ne soient expirés ou révoqués.

Dernière mise à jour: 22 septembre 2023