## 1. OBJET

Les présentes conditions ont pour objet de préciser les conditions générales de vente et d'utilisation (CGVU) d'un CERTIFICAT délivré par CERTIGNA ainsi que les engagements et obligations respectifs des PARTIES liées aux présentes. Les CGVU découlent d'une Politique de Certification (PC) associée au CERTIFICAT délivré. Chaque PC est publiée en ligne et est identifiée par un identifiant unique OID dont découlent les OID des différents CERTIFICATS associés. Les CERTIFICATS couverts par le présent CONTRAT sont listés ci-dessous sous la représentation suivante :

| **NOM DE L'AUTORITE DE CERTIFICATION** | **OID de la PC** |
|---|---|
| Type de certificat : niveau(x) de qualification | OID du certificat |
| Lien vers la PC associée | **Profil du concerné** |

Les CERTIFICATS couverts par le présent CONTRAT sont les suivants :

| | |
|---|---|
| **CERTIGNA IDENTITY CA** | **1.2.250.1.177.2.3.1.** |
| Chiffrement RGS * + LCP | 1.2.250.1.177.2.3.1.1.1 |
| Chiffrement RGS * + LCP | 1.2.250.1.177.2.3.1.3.1 |
| Authentification & signature RGS * + LCP | 1.2.250.1.177.2.3.1.2.1 |
| Authentification & signature RGS * + LCP | 1.2.250.1.177.2.3.1.4.1 |
| http://politique.certigna.fr/PCcertignaidentityca.pdf | **PORTEUR** |
| **CERTIGNA IDENTITY PLUS CA** | **1.2.250.1.177.2.4.1.** |
| Authentification & signature RGS ** + QCP-n-qscd | 1.2.250.1.177.2.4.1.1.1 |
| Authentification RGS *** + QCP-n-qscd | 1.2.250.1.177.2.4.1.2.1 |
| Signature RGS *** + QCP-n-qscd | 1.2.250.1.177.2.4.1.3.1 |
| Authentification & signature RGS ** + QCP-n-qscd | 1.2.250.1.177.2.4.1.4.1 |
| Authentification RGS *** + QCP-n-qscd | 1.2.250.1.177.2.4.1.5.1 |
| Signature RGS *** + QCP-n-qscd | 1.2.250.1.177.2.4.1.6.1 |
| http://politique.certigna.fr/PCcertignaidentityplusca.pdf | **PORTEUR** |
| **CERTIGNA ENTITY CA** | 1.2.250.1.177.2.6.1 |
| Cachet de mails et documents RGS * + LCP | 1.2.250.1.177.2.6.1.1.1 |
| Cachet de mails et documents RGS ** + QCP-l-qscd | 1.2.250.1.177.2.6.1.4.1 |
| Cachet de mails et documents RGS ** | 1.2.250.1.177.2.6.1.42.1 |
| Cachet de mails et documents QCP-l-qscd | 1.2.250.1.177.2.6.1.41.1 |
| Cachet de mails et documents QCP-l | 1.2.250.1.177.2.6.1.7.1 |
| Cachet de mails et documents QCP-l + DSP2 | 1.2.250.1.177.2.6.1.8.1 |
| Cachet de jetons d'horodatage RGS * + LCP | 1.2.250.1.177.2.6.1.3.1 |
| Cachet de jetons d'horodatage RGS ** + QCP-l-qscd | 1.2.250.1.177.2.6.1.6.1 |
| http://politique.certigna.fr/PCcertignaentityca.pdf | **RC** |
| **CERTIGNA ENTITY CODE SIGNING CA** | 1.2.250.1.177.2.8.1 |
| Cachet de code RGS * + LCP | 1.2.250.1.177.2.8.1.1.1 |
| Cachet de code RGS ** + QCP-l-qscd | 1.2.250.1.177.2.8.1.2.1 |
| http://politique.certigna.fr/PCcertignaentitycsca.pdf | **RC** |
| **FR03** | **1.2.250.1.177.2.2.1** |
| Cachet de documents (2D-DOC) | 1.2.250.1.177.2.2.1.1 |
| http://politique.certigna.fr/PCfr03.pdf | **RC** |
| **CERTIGNA SERVICES CA** | **1.2.250.1.177.2.5.1** |
| Authentification serveur RGS * + OVCP | 1.2.250.1.177.2.5.1.1.1 |
| Authentification client RGS * + OVCP | 1.2.250.1.177.2.5.1.2.1 |
| Authentification serveur QCP-w | 1.2.250.1.177.2.5.1.3.1 |
| http://politique.certigna.fr/PCcertignaservicesca.pdf | **RC** |
| **CERTIGNA WILD CA** | **1.2.250.1.177.2.7.1** |
| Authentification client/serveur OVCP | 1.2.250.1.177.2.7.1.1.1 |
| Authentification client/serveur wildcard OVCP | 1.2.250.1.177.2.7.1.2.1 |
| http://politique.certigna.fr/PCcertignawildca.pdf | **RC** |

## 2. DÉFINITIONS

Les termes ci-dessous énoncés, utilisés tout au long des présentes CGVU, et débutant par une majuscule ont, sauf stipulation contraire, la signification suivante qu'ils soient indifféremment utilisés au singulier ou au pluriel :

- **AC** : Autorité de Certification de la société CERTIGNA, délivrant le CERTIFICAT.
- **AC RACINE** : Autorité de plus haut niveau de l'Infrastructure de Gestion de Clé (IGC) de CERTIGNA qui certifie les AC EMETTRICES.
- **AC EMETTRICE** : Autorité dont le CERTIFICAT a été signé par l'AC RACINE. L'AC est une autorité émettrice dans l'IGC Certigna.
- **AE** : Autorité d'Enregistrement de la société CERTIGNA, contrôlant les demandes de CERTIFICAT et les éventuelles demandes de REVOCATION.
- **AUTORITE D'ENREGISTREMENT DELEGUEE (AED)** : Entité tierce externe à l'IGC avec laquelle CERTIGNA a conclu un contrat de délégation par lequel il sous-traite une partie de l'activité de l'AE, à savoir, la collecte et le contrôle des dossiers d'enregistrement, l'identification des demandeurs de CERTIFICAT et la soumission des demandes de REVOCATION.
- **CACHET** : Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières.
- **CERTIFICAT** : Certificat électronique constitué d'un fichier de données électroniques signé numériquement, conforme à la norme X.509 v3, contenant des informations :
  - sur le SERVEUR dont est responsable le RC pour un CERTIFICAT d'authentification serveur et/ou client ;
  - sur le service de CACHET dont est responsable le RC pour un CERTIFICAT de CACHET ;
  - sur le PORTEUR pour un CERTIFICAT de chiffrement ou d'authentification et/ou de signature.
- **CONTRAT** : Relations entre l'AC et le PORTEUR ou le RC encadrées par les présentes CGVU expressément acceptées par le PORTEUR ou le RC lors de chaque DEMANDE de CERTIFICAT. Sont également inclus dans le CONTRAT l'ensemble des documents auxquels les présentes CGVU font référence notamment la Politique d'utilisation des données personnelles disponible sur le site Certigna.com.
- **DEBLOCAGE** : Opération consistant à réinitialiser le code PIN d'un **SUPPORT CRYPTOGRAPHIQUE** bloqué suite à la saisie de 3 codes PIN incorrects ;
- **DEMANDE DE CERTIFICAT** : Ensemble constitué du formulaire de demande signé (acceptant les présentes CGVU) accompagné des pièces justificatives, et de la requête générée informatiquement.
- **INFRASTRUCTURE DE GESTION DE CLE (IGC)** : désigne l'ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une AC, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, …
- **LCR** : Liste des CERTIFICATS révoqués.
- **MANDATAIRE DE CERTIFICATION (MC)** : Personne désignée et placée sous la responsabilité de l'entité cliente. Elle est en relation directe avec l'AE et assure pour elle un certain nombre de vérifications concernant l'identité du PORTEUR ou du RC de cette entité.
- **OID** : Identifiant d'objet (Object IDentifier).
- **OCSP STAPLING** : Configuration du système de vérification de l'état du CERTIFICAT afin qu'il assure le rôle de proxy pour l'interrogation OCSP et cela afin de réduire drastiquement le nombre de requêtes transmises au répondeur OCSP de l'AC.
- **PARTIE(S)** : Individuellement le PORTEUR ou le RC ou l'AC, et collectivement, l'AC et le PORTEUR ou l'AC et le RC.
- **PORTEUR** : Personne physique pour laquelle la demande de CERTIFICAT a été acceptée et traitée par l'AC, qui est responsable de ce CERTIFICAT et de la clé privée correspondante.
- **RC** : Personne physique en charge et responsable du CERTIFICAT utilisé pour le SERVEUR ou le service de CACHET et de la clé privée associée.
- **REFABRICATION** : Opération consistant à émettre un nouveau CERTIFICAT en remplacement d'un existant, avec exactement les mêmes informations mais une bi-clé différente (suite à la perte du certificat ou du mot de passe).
- **REVOCATION** : Opération consistant à anticiper la fin de validité d'un CERTIFICAT initialement prévue et dont la date est inscrite dans le CERTIFICAT.
- **SERVEUR** : serveur informatique hébergeant un service sécurisé par un CERTIFICAT, permettant l'authentification de ce service par des UTILISATEURS et la sécurisation des échanges avec ces derniers.
- **SUPPORT CRYPTOGRAPHIQUE** : dispositif au format clé USB ou carte à puce ou module cryptographique.
- **UTILISATEUR** : Utilisateur d'un CERTIFICAT. Il peut s'agir de :
  - Pour un CERTIFICAT de chiffrement, il peut s'agir d'un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du porteur du certificat, ou encore d'une personne qui émet un message chiffré à l'intention du porteur du certificat électronique.
  - Pour un CERTIFICAT d'Authentification, il peut s'agir :
    - D'un service en ligne qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le PORTEUR du CERTIFICAT ;
    - D'un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine.
  - Pour un CERTIFICAT de signature, il peut s'agir :
    - D'un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le PORTEUR du CERTIFICAT ;
    - D'un usager qui signe électroniquement un document ou un message ;
    - D'un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le PORTEUR du CERTIFICAT sur ce message ou sur ces données.
  - Pour un CERTIFICAT d'Authentification et de signature, il peut s'agir des mêmes utilisateurs que pour un certificat d'authentification ou de signature.
  - Pour un CERTIFICAT de CACHET :
    - Un usager destinataire de données signées par un service applicatif de CACHET et qui utilise le CERTIFICAT ainsi qu'un module de vérification de CACHET afin d'authentifier l'origine de ces données transmises.
    - Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le CERTIFICAT et un module de vérification de CACHET afin d'authentifier l'origine de ces données transmises.

    Un service applicatif qui signe des données électroniques.
  - Pour un CERTIFICAT d'Authentification de serveur, d'une personne accédant à un SERVEUR et qui utilise le CERTIFICAT du SERVEUR et un module de vérification

d'authentification afin d'authentifier le SERVEUR auquel il accède, qui est identifié dans le CERTIFICAT du SERVEUR, afin d'établir une clé de session partagée entre son poste et le SERVEUR ;

- Pour un CERTIFICAT d'Authentification client, d'un service applicatif accédant à un SERVEUR et qui utilise un CERTIFICAT et un applicatif de vérification d'authentification afin d'authentifier le SERVEUR auquel il accède, qui est identifié dans le CERTIFICAT, et afin d'établir une clé de session partagée entre les deux SERVEURS.

## 3. LIVRAISON, GARANTIE ET CONFORMITÉ NORMATIVE

**3.1 Livraison et garanties**

Tout CERTIFICAT commandé doit être accepté par le PORTEUR ou le RC sur l'espace client qu'il s'est créé depuis le site de l'AC ou de l'un de ses AED. Avant la génération du CERTIFICAT, Le PORTEUR ou le RC doit vérifier que les informations énoncées dans la DEMANDE DE CERTIFICAT sont exactes. A défaut, le PORTEUR ou le RC doit prendre contact avec un membre du personnel de l'AC ou de l'AED. S'il s'agit de l'AC, soit par téléphone au 0 806 115 115 (service gratuit coût d'un appel local), soit par email à l'adresse suivante : contact@certigna.fr. Le support téléphonique est disponible du lundi au vendredi, sauf jours fériés, de 9h à 18h sans interruption. Le PORTEUR ou le RC est conscient qu'en cas d'erreur lors de la commande dans la nature même du CERTIFICAT, aucune modification ne pourra être faite par l'AC et une nouvelle DEMANDE DE CERTIFICAT devra être réalisée par le PORTEUR ou le RC. Si un paiement avait déjà été effectué, l'AC ne serait tenue à aucun remboursement.

Une fois la DEMANDE DE CERTIFICAT validée, le CERTIFICAT est généré. Le PORTEUR ou le RC est alors amené à confirmer l'exactitude desdites informations, ce qui vaut acceptation du CERTIFICAT. A ce stade, aucune modification des informations ne peut être effectuée par l'AC. Il est donc de la responsabilité du PORTEUR ou du RC de bien vérifier l'exactitude de ses informations la première fois que cela lui est demandé. A défaut, le PORTEUR ou le RC devra faire une nouvelle DEMANDE DE CERTIFICAT et le CERTIFICAT généré ne donnera lieu à aucun remboursement.

Une fois le CERTIFICAT accepté, celui-ci est mis à la disposition du PORTEUR ou du RC soit depuis son espace client, soit sur un SUPPORT CRYPTOGRAPHIQUE. L'installation du CERTIFICAT se fait sous la seule responsabilité du PORTEUR ou du RC. En cas de difficulté quelconque pendant cette dernière phase, le PORTEUR ou le RC peut contacter l'AC ou l'AED au numéro de téléphone et l'adresse email de l'AC indiqués précédemment ou aux coordonnées disponibles sur le site de l'AED. L'AC ne garantit pas le fonctionnement du CERTIFICAT dans le cas d'une utilisation en dehors des usages prévus à l'article 10 des présentes.

**3.2 Conformité normative**

Le CERTIFICAT est émis en conformité avec un ou plusieurs des référentiels suivants :

- Les exigences de la PC Type « *Certificats électroniques de Services Applicatifs* » pour un usage de cachet ou d'authentification de client/serveur ou de la PC Type « *Certificats électroniques de Personnes* » pour un usage de chiffrement, d'authentification et/ou de signature du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- Le règlement européen eIDAS (EU) N°910/2014 ;
- Les exigences de l'ETSI EN 319 411-1 niveau LCP, NCP, NCP+, DVCP, OVCP ou EVCP ;
- Les exigences de l'ETSI EN 319 411-2 niveau QCP, QCP-n, QCP-l, QCP-n-qscd or QCP-l-qscd;
- Les exigences du document « Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates » du CA/BROWSER FORUM.
- Les exigences du document « Guidelines For The Issuance and Management Of Extended Validation Certificates » du CA/BROWSER FORUM pour les CERTIFICATS d'authentification serveur qualifié ;

Les niveaux de qualifications et de certifications obtenus pour chaque CERTIFICAT sont décrits dans les tableaux ci-dessous.

| CERTIGNA IDENTITY CA | | RGS | ETSI |
|---|---|---|---|
| Chiffrement | 1.2.250.1.177.2.3.1.1.1 | * | LCP |
| Chiffrement | 1.2.250.1.177.2.3.1.3.1 | * | LCP |
| Authentification & signature | 1.2.250.1.177.2.3.1.2.1 | * | LCP |
| Authentification & signature | 1.2.250.1.177.2.3.1.4.1 | * | LCP |

| CERTIGNA IDENTITY PLUS CA | | RGS | ETSI |
|---|---|---|---|
| Authentification & signature | 1.2.250.1.177.2.4.1.1.1 | ** | QCP-n-qscd |
| Authentification | 1.2.250.1.177.2.4.1.2.1 | *** | QCP-n-qscd |
| Signature | 1.2.250.1.177.2.4.1.3.1 | *** | QCP-n-qscd |
| Authentification & signature | 1.2.250.1.177.2.4.1.4.1 | ** | QCP-n-qscd |
| Authentification | 1.2.250.1.177.2.4.1.5.1 | *** | QCP-n-qscd |
| Signature | 1.2.250.1.177.2.4.1.6.1 | *** | QCP-n-qscd |

| CERTIGNA ENTITY CA | | RGS | ETSI |
|---|---|---|---|
| Cachet mails et documents | 1.2.250.1.177.2.6.1.1.1 | * | LCP |
| Cachet mails et documents | 1.2.250.1.177.2.6.1.4.1 | ** | QCP-l-qscd |
| Cachet mails et documents | 1.2.250.1.177.2.6.1.42.1 | ** | |
| Cachet mails et documents | 1.2.250.1.177.2.6.1.41.1 | | QCP-l-qscd |
| Cachet mails et documents | 1.2.250.1.177.2.6.1.7.1 | | QCP-l |
| Cachet mails et documents | 1.2.250.1.177.2.6.1.8.1 | | QCP-l |
| Cachet jetons d'horodatage | 1.2.250.1.177.2.6.1.3.1 | * | LCP |
| Cachet jetons d'horodatage | 1.2.250.1.177.2.6.1.6.1 | ** | QCP-l-qscd |

| CERTIGNA ENTITY CODE SIGNING CA | | RGS | ETSI |
|---|---|---|---|
| Cachet de code | 1.2.250.1.177.2.8.1.1.1 | * | LCP |
| Cachet de code | 1.2.250.1.177.2.8.1.2.1 | ** | QCP-l-qscd |

| FR03 | | RGS | ETSI |
|---|---|---|---|
| Cachet de 2D-DOC | 1.2.250.1.177.2.2.1.1 | * | NCP+ |

| CERTIGNA SERVICES CA | | RGS | ETSI |
|---|---|---|---|
| Authentification serveur | 1.2.250.1.177.2.5.1.1.1 | * | OVCP |
| Authentification client | 1.2.250.1.177.2.5.1.2.1 | * | OVCP |
| Authentification serveur | 1.2.250.1.177.2.5.1.3.1 | | QCP-w |

| CERTIGNA WILD CA | | RGS | ETSI |
|---|---|---|---|
| Authentification client/serveur | 1.2.250.1.177.2.7.1.1.1 | | OVCP |
| Authentification client/serveur wildcard | 1.2.250.1.177.2.7.1.2.1 | | OVCP |

La conformité du CERTIFICAT peut être vérifiée au travers de la liste publiée par l'organisme de certification LSTI sur son site lsti.fr dans la section « Certification/PSCe ».

## 4. DURÉE

Le CONTRAT est conclu pour une durée choisie lors de la DEMANDE DE CERTIFICAT. Cette durée démarre le jour de la délivrance du CERTIFICAT par l'AC et ne peut excéder :

- Huit cents vingt-cinq (825) jours pour un CERTIFICAT d'authentification serveur et/ou client ;
- Trois (3) ans pour un CERTIFICAT pour un professionnel ;
- Cinq (5) ans pour un CERTIFICAT pour un particulier ;

Le présent CONTRAT prend automatiquement fin dès révocation ou expiration du CERTIFICAT, sauf pour les clauses qui ont vocation à perdurer au-delà.

## 5. TARIFS ET CONDITIONS DE REMBOURSEMENT

**5.1. Tarifs**

Sauf accord écrit et préalable de l'AC, les conditions tarifaires et de paiement sont les suivantes :

- Le prix de vente du CERTIFICAT est celui fixé dans la grille tarifaire disponible sur demande auprès du service commercial de CERTIGNA ou de son AED le cas échéant,
- Le prix de vente du CERTIFICAT est à payer lors de la DEMANDE DE CERTIFICAT par l'un des moyens suivants :
  - carte bancaire sur le site https://certigna.fr ;
  - virement bancaire, en joignant le récépissé fourni par la banque ;
  - chèque libellé à l'ordre de CERTIGNA ;
  - mandat administratif, pour les établissements publics uniquement, en joignant un bon de commande au nom de l'Établissement.
- La refabrication d'un CERTIFICAT, contenant les mêmes informations validées, est gratuite durant les 3 mois qui suivent la délivrance du CERTIFICAT par l'AC ;
- Le déblocage du SUPPORT CRYPTOGRAPHIQUE dans lequel est fourni le CERTIFICAT le cas échéant, est une prestation facturée ;

Tous les prix sont exprimés hors taxes et majorés de la TVA ou autre taxe applicable au taux en vigueur à la date de facturation. Tous les prix s'entendent frais d'acheminement compris, sauf si une information contraire est communiquée lors de la DEMANDE DE CERTIFICAT. Le PORTEUR ou le RC ne peut en aucun cas compenser, réduire ou modifier les prix ni en suspendre le paiement de manière anticipée.

Sauf accord écrit et préalable de l'AC ou de l'AED, tout CERTIFICAT dont le prix de vente n'a pas été payé intégralement, pourra soit ne pas être délivré, soit être révoqué après sa délivrance par l'AC. Conformément à l'article L.441-10 du Code de commerce, en cas de non-paiement à la date d'échéance indiquée sur la facture, sans obligation d'envoi d'une relance, seront appliquées des pénalités de retard calculées au taux de 3 fois le taux d'intérêt légal en vigueur au jour d'exigibilité de la facture, ainsi qu'une indemnité forfaitaire de 40€ pour frais de recouvrement.

**5.2. Conditions de remboursement**

La commande de CERTIFICAT ne peut être annulée dès lors que la DEMANDE de CERTIFICAT a été faite. Ainsi, tout CERTIFICAT émis ne peut faire l'objet d'une demande de remboursement notamment suite à des difficultés de mise en œuvre liées notamment à l'environnement technique d'exploitation du CERTIFICAT (Ex : non-conformité des logiciels ou matériels stockant et utilisant le CERTIFICAT avec les standards et normes en vigueur). Toutefois, dans l'hypothèse où le CERTIFICAT ne correspond pas à la DEMANDE DE CERTIFICAT suite à une erreur exclusivement imputable à l'AC, l'AC s'engage à fournir un CERTIFICAT conforme, ou le cas échéant s'il est dans l'incapacité de le faire, de procéder au remboursement des sommes déjà versées au titre du CONTRAT.

## 6. OBLIGATIONS DU PORTEUR OU DU RC

Le PORTEUR ou le RC a le devoir de :

- Effectuer sa DEMANDE DE CERTIFICAT en suivant toutes les étapes de la procédure figurant sur le site https://www.certigna.fr.
- Communiquer des informations exactes et à jour pour la DEMANDE DE CERTIFICAT ou son renouvellement ;

- Transmettre à l'AE, le cas échéant à l'AED, ou à un MC de son entité, en main propre ou par voie postale, le formulaire d'inscription généré lors de la DEMANDE DE CERTIFICAT en ligne sur le site https://www.certigna.fr ou sur le site de l'AED le cas échéant, le paiement, ainsi que les pièces justificatives.
- Générer la bi-clé associé au CERTIFICAT dans un dispositif qui est conforme aux exigences de sécurité du chapitre 11 de la Politique de Certification associée au CERTIFICAT.
  Des justificatifs attestant de la conformité du dispositif pourront être demandés par l'AC lors de la DEMANDE DE CERTIFICAT (cas notamment d'un CERTIFICAT de CACHET). Ces justificatifs seront à minima la facture d'achat du dispositif et des photos/impressions d'écran des caractéristiques matérielles et logicielles du dispositif et du numéro de série associé. L'AC se réserve le droit de refuser la DEMANDE DE CERTIFICAT en l'absence de justificatifs ou s'il était avéré que ce dispositif ne réponde pas à ces exigences.
- Dans le cas où l'AC serait informée ou aurait identifiée la perte de la conformité du dispositif, l'AC demandera au PORTEUR ou RC les preuves attestant que la bi-clé est toujours stockée dans un dispositif répondant aux exigences du chapitre 11 de la Politique de Certification associée au CERTIFICAT. Le PORTEUR ou le RC s'engage à fournir ces preuves (Ex : Facture d'achat d'un nouveau dispositif, Procès-verbal de cérémonie des clés en cas de migration des clés, Procès-verbal de mise à jour du dispositif pour le maintien de la certification, etc.) dans un délai de quinze (15) jours suivants la demande par l'AC. Dans le cas où aucune preuve ne seraient fournies ou que ces dernières ne permettraient pas de déterminer si les conditions de stockage de la bi-clé, et de transfert dans un autre dispositif le cas échéant, répondent aux exigences de la Politique de Certification, l'AC se donne le droit de révoquer le CERTIFICAT.
- Informer l'AE en cas de non-réception d'un e-mail confirmant la prise en compte de la DEMANDE DE CERTIFICAT ou de REVOCATION ;
- Suite à la réception d'un e-mail de l'AE signalant la non-conformité de la DEMANDE DE CERTIFICAT ou que le dossier est incomplet, d'effectuer les modifications sous sept (7) jours calendaires après la réception de cet e-mail ;
- Télécharger le CERTIFICAT généré, mis à disposition sur son espace client le cas échéant, dans les trente (30) jours qui suivent la validation de la DEMANDE DE CERTIFICAT qui est notifiée par e-mail au PORTEUR ou au RC. Au-delà de ce délai, le CERTIFICAT est révoqué automatiquement par l'AE.
- Accepter explicitement le CERTIFICAT après sa génération et depuis son espace client CERTIGNA ou celui de son AED le cas échéant. Cette acceptation peut également être opérée par l'envoi d'un courrier papier signé par le PORTEUR ou le RC sur demande expresse de l'AE. En cas de non-acceptation explicite, le CERTIFICAT est automatiquement révoqué par l'AE ;
- Protéger la clé privée associée au CERTIFICAT dont il a la responsabilité par des moyens appropriés à son environnement et conformément aux exigences du chapitre 11 de la Politique de Certification associée ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du SERVEUR pour les CERTIFICAT d'authentification serveur/client ;
- Respecter les conditions d'usages du CERTIFICAT et de la clé privée associée citées au chapitre 10 de ce document ;
- Informer l'AC de toute modification concernant les informations contenues dans le CERTIFICAT ;
- Faire, sans délai, une demande de REVOCATION du CERTIFICAT dont il est responsable auprès de l'AE, de l'AED auprès de laquelle la DEMANDE DE CERTIFICAT a été effectuée ou le cas échéant du MC de l'entité, lorsque l'une des causes de REVOCATION du chapitre 9 est rencontrée ;
- Prendre toutes les mesures propres à assurer la sécurité du ou des dispositifs sur lesquels est installé le CERTIFICAT. Le PORTEUR ou le RC est le seul responsable de l'installation du CERTIFICAT ;
- Ne plus utiliser un CERTIFICAT et à supprimer la bi-clé associée suite à l'expiration ou la REVOCATION de ce CERTIFICAT ;
- Informer l'AE de son départ de l'entité ou de son changement de responsabilités et du besoin d'enregistrer un nouveau PORTEUR ou RC ;
- Vérifier l'adéquation à son besoin du CERTIFICAT et de ses caractéristiques ;
- S'assurer que les prérequis matériels et/ou logiciels préconisés par l'AC sont remplis en vue de l'installation le cas échéant et de l'utilisation du CERTIFICAT ;
- Disposer de toutes les compétences et moyens nécessaires pour utiliser les CERTIFICATS ;
- Mettre en œuvre des mesures permettant d'empêcher toute personne non autorisée d'accéder physiquement au dispositif stockant la clé privée et le CERTIFICAT ;
- Prévenir sans délai la personne en charge de la sécurité des systèmes d'information de son entité (exemple : RSSI) en cas de perte ou de vol du dispositif stockant les clés et le CERTIFICAT ; et
- Pour les applications jugées les plus critiques au niveau métier, mettre en place des mesures permettant de détecter des transactions potentiellement frauduleuses (incohérence des données métiers signés, etc.) et de prévoir, le cas échéant, une procédure alternative.
- S'il s'agit d'un CERTIFICAT d'authentification serveur et/ou client, et dans le cas où pour un ou plusieurs noms de domaine à intégrer dans le CERTIFICAT, l'option « DNS CAA » est activée, le RC doit mettre à jour les enregistrements DNS associés afin d'y faire figurer l'AC, et ce préalablement à la demande de CERTIFICAT.

## 7. OBLIGATIONS DE L'AC ET DE L'AE

L'AC est tenue à une obligation de moyens pour toutes les obligations relatives à la gestion du cycle de vie du CERTIFICAT qu'elle émet. L'AC s'engage à :

- Pouvoir démontrer, aux UTILISATEURS, qu'elle a émis le CERTIFICAT pour un PORTEUR ou un service de CACHET ou un SERVEUR donné et que le PORTEUR ou le RC correspondant a accepté le CERTIFICAT ;
- Prendre toutes les mesures raisonnables pour s'assurer que les PORTEURS et les RC sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des CERTIFICATS ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC ;
- Fournir un service de maintenance technique par téléphone aux heures ouvrées ;
- Fournir un service de consultation en ligne sur le site https://www.certigna.fr permettant à tout moment aux tiers de vérifier la validité du CERTIFICAT émis par l'AC (cf. chapitre 12) ;
- Réaliser toute collecte et tout usage de données à caractère personnel dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, et de la Politique d'utilisation des données personnelles disponible sur le site certigna.com ;
- Mettre en œuvre et suivre, lors de l'émission d'un CERTIFICAT, les exigences décrites aux chapitres 3.2 et 3.3 de la PC associée pour vérifier que l'organisation rattachée au PORTEUR ou au service de CACHET ou au SERVEUR a autorisé la délivrance du CERTIFICAT, et que le RC est autorisé à demander le CERTIFICAT au nom de l'organisation ;
- Mettre en œuvre et suivre, lors de l'émission d'un CERTIFICAT, les exigences décrites aux chapitres 3.2 et 3.3 de la PC pour vérifier que les informations contenues dans le CERTIFICAT sont exactes.
- Mettre en œuvre et suivre, lors de l'émission d'un CERTIFICAT, les exigences décrites aux chapitres 3.2 et 3.3 de la PC pour vérifier l'identité de l'organisation, de son représentant légal et du PORTEUR ou RC désigné ;
- Si l'AC et l'organisation qui demande le CERTIFICAT ne sont pas affiliées, ces parties s'engagent sur un accord de souscription juridiquement valide et exécutoire ;
- Si l'AC et l'organisation qui demande le CERTIFICAT sont la même entité ou sont affiliées, le représentant de l'organisation qui demande le CERTIFICAT a reconnu les présentes CGVU ;
- Mettre à disposition du public 24h/24, 7j/7 les informations sur l'état (valide ou révoqué) des CERTIFICATS non expirés ; et
- Révoquer un CERTIFICAT pour l'une des raisons spécifiées à l'article 9 ;
- S'il s'agit d'un CERTIFICAT d'authentification serveur et/ou client, mettre en œuvre et suivre, lors de la délivrance d'un CERTIFICAT, les exigences décrites aux chapitres 3.2 et 3.3 de la PC associée pour vérifier que le PORTEUR ou le RC a le droit d'utiliser ou de contrôler le(s) nom(s) de domaine indiqué(s) dans les champs « commonName » et « subjectAltName » du CERTIFICAT (ou uniquement dans le cas où les droits d'utilisation ou de contrôle des noms de domaine ont été délégués par une personne disposant de ces droits) ;

L'AE s'engage à :

- Vérifier et à valider les dossiers de DEMANDE DE CERTIFICAT et de REVOCATION de CERTIFICAT ;
- Générer et mettre à la disposition du PORTEUR ou du RC le CERTIFICAT dans un délai trente de (30) jours dans le cas où la DEMANDE DE CERTIFICAT est conforme et le dossier de demande complet ; et
- Révoquer le CERTIFICAT sous 24 heures dans le cas où la demande de REVOCATION est conforme et le demandeur est authentifié et autorisé.

## 8. PUBLICATION DES CERTIFICATS

Le CERTIFICAT ne fait pas l'objet de publication par l'AC hormis s'il s'agit d'un CERTIFICAT de CACHET de documents de type 2D-DOC. Dans ce cas le RC accepte explicitement que le CERTFICAT émis par l'AC fasse l'objet d'une publication dans un annuaire à l'adresse suivante : http://certificates.certigna.fr.

## 9. RÉVOCATION

Les circonstances suivantes peuvent être à l'origine de la REVOCATION du CERTIFICAT :

- Le PORTEUR ou le RC, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la REVOCATION du CERTIFICAT (notamment dans le cas d'une destruction ou altération de la clé privée et/ou de son support) ;
- Le représentant légal de l'entité à laquelle le PORTEUR, le SERVEUR ou le service de CACHET appartient le cas échéant, informe l'AC que la DEMANDE DE CERTIFICAT originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
- L'AC obtient la preuve que la clé privée correspondant à la clé publique du CERTIFICAT est suspectée de compromission, est compromise, est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée),
- S'agit d'un CERTIFICAT d'authentification serveur et/ou client, et que l'AC obtient la preuve que la validation de l'autorisation du domaine ou du contrôle d'un ou plusieurs FQDN dans le CERTIFICAT n'est pas fiable.

L'AC révoquera un CERTIFICAT sous 5 jours dans une ou plusieurs des situations suivantes :

- Le CERTIFICAT n'est plus conforme aux exigences des chapitres 6.1.5 et 6.1.6 de la PC ;
- L'AC obtient la preuve que l'usage du CERTIFICAT est détourné ;
- L'AC est informée que le PORTEUR ou le RC n'a pas respecté toute ou partie des dispositions du CONTRAT ou a violé une ou plusieurs de ses obligations en vertu des présentes CGVU ;
- S'agit d'un CERTIFICAT d'authentification serveur et/ou client et que l'AC est informée de toute circonstance indiquant que l'utilisation d'un nom de domaine dans le CERTIFICAT n'est plus autorisée légalement (Ex : un tribunal ou un arbitre a révoqué le droit d'un titulaire de nom de domaine d'utiliser le nom de domaine, une licence ou un accord de services entre le titulaire et le demandeur est terminée, ou le titulaire n'a pas pu renouveler le nom de domaine) ;
- Les informations du PORTEUR, du service de CACHET ou du SERVEUR figurant dans le CERTIFICAT ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le CERTIFICAT (par exemple, modification de l'identité du PORTEUR, du service de CACHET ou du SERVEUR), ceci avant l'expiration normale du CERTIFICAT ;

- L'AC est informée que le CERTIFICAT n'a pas été émis en conformité avec les exigences et pratiques formulées dans la PC ou la DPC associée ;
- L'AC détecte ou est informée que les informations apparaissant dans le CERTIFICAT sont inexactes ou trompeuses ;
- Le droit de l'AC de délivrer des certificats sous les exigences du CA/Browsers Forum expire ou est révoqué ou terminé, à moins que l'AC ait prévu de continuer le maintien des services de CRL/OCSP ;
- La révocation est requise par la PC ou la DPC correspondante ;
- L'AC est informée par une démonstration ou une méthode éprouvée que la clé privée est compromise ou il y une preuve évidente que la méthode spécifique pour générer la clé privée était défectueuse. Des méthodes ont été développées qui peuvent aisément permettre de la calculer sur la base de la clé publique (telle que la clé vulnérable de Debian, cf. http://wiki.debian.org/SSLkeys),
- Le PORTEUR ou le RC, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC ou de la DPC;
- L'AC cesse ses activités pour quelque raison que ce soit et n'a pas pris de dispositions pour qu'une autre AC assure le relai en cas de REVOCATION du CERTIFICAT ;
- Le CERTIFICAT de signature de l'AC est révoqué, ce qui entraîne la REVOCATION de tous les CERTIFICATS en cours de validité signés par la clé privée correspondante ;
- Le contenu ou le format des CERTIFICATS présente un risque inacceptable pour les fournisseurs de logiciels applicatifs ou les utilisateurs (Ex : le CA/Browser Forum peut déterminer qu'un algorithme ou une clé de chiffrement/signature obsolète présente un risque inacceptable et que ces CERTIFICATS doivent être révoqués et remplacés par l'AC sous un délai donné.
- L'arrêt définitif du service de CACHET ou du SERVEUR ou la cessation d'activité de l'entité du RC ;
- Le départ de la société du PORTEUR ou la cessation d'activité de l'entité de rattachement du PORTEUR ;
- Une erreur (intentionnelle ou non) a été détectée dans la DEMANDE DE CERTIFICAT et le dossier d'enregistrement correspondant ;
- Pour des raisons techniques (échec de l'envoi du CERTIFICAT, …).

La demande de REVOCATION peut être effectuée par :

- Le PORTEUR ou le RC, un représentant légal de l'entité rattachée au CERTIFICAT, ou le cas échéant un MC de cette entité, et/ou
- L'AC, l'AE ou un AED.

La demande de REVOCATION peut être effectuée :

- Par courrier signé, accompagné de la photocopie d'une pièce d'identité officielle du demandeur ;
- En ligne, sur le site https://www.certigna.fr ou de l'AED, depuis l'espace client du PORTEUR ou du RC ou du MC le cas échéant.

## 10. CONDITIONS D'USAGE DU CERTIFICAT ET DE LA CLÉ PRIVÉE ASSOCIÉE

- Pour un CERTIFICAT de chiffrement, les usages sont :
  - Déchiffrement : à l'aide de sa clé privée, un porteur déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clé publique figurant dans le CERTIFICAT ;
  - Chiffrement : à l'aide de la clé publique du destinataire, une personne chiffre des données.
- Pour un CERTIFICAT d'Authentification et/ou de signature, les usages sont :
  - Authentification des porteurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.
  - Signature électronique de données. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.
- Pour un CERTIFICAT de cachet pour la signature de mails et de documents, les usages sont la signature électronique de données et la vérification de signature électronique. Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, un mail, un document ou encore une archive.
- Pour un CERTIFICAT de cachet pour la signature de jeton d'horodatage, les usages sont la signature électronique de jeton d'horodatage et la vérification de signature électronique.
- Pour un CERTIFICAT de cachet de documents 2D-DOC, les usages sont la signature électronique de données contenues dans un 2D-DOC et la vérification de la signature électronique. Le type de données signées doit être conforme à celui qui a été déclaré par le RC lors de la DEMANDE DE CERTIFICAT.
- Pour un CERTIFICAT d'Authentification serveur et/ou client, les usages sont l'authentification du SERVEUR auprès d'autres SERVEURS ou de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

En cas de non-respect de ces usages, la responsabilité du PORTEUR ou du RC ou de l'entité à laquelle le CERTIFICAT est rattaché pourrait être engagée.

## 11. OBLIGATIONS DES UTILISATEURS

Les UTILISATEURS doivent :

- Respecter les usages autorisés du CERTIFICAT et de la clé privée associée. Dans le cas contraire, leur responsabilité pourrait être engagée ;
- Vérifier, avant son utilisation, l'état des CERTIFICATS de l'ensemble de la chaîne de certification correspondante via les moyens offerts pour la vérification des CERTIFICATS cités ci-dessous ; et
- Si le CERTIFICAT de l'AC racine CERTIGNA n'est pas installé sur le poste de l'UTILISATEUR, ce dernier doit le télécharger à partir du site https://www.certigna.fr , précisément aux adresses suivantes :
  - http://autorite.certigna.fr/ACcertignarootca.crt ;
  - http://autorite.dhimyotis.com/ACcertignarootca.crt.

Le CERTIFICAT de chaque Autorité de Certification CERTIGNA peut être téléchargé depuis les adresses suivantes :

**CERTIGNA IDENTITY CA**
http://autorite.certigna.fr/identca.crt
http://autorite.dhimyotis.com/identca.crt

**CERTIGNA IDENTITY PLUS CA**
http://autorite.certigna.fr/identityplusca.crt
http://autorite.dhimyotis.com/identittyplusca.crt

**CERTIGNA ENTITY CA**
http://autorite.certigna.fr/entityca.crt
http://autorite.dhimyotis.com/entityca.crt

**CERTIGNA ENTITY CODE SIGNING CA**
http://autorite.certigna.fr/entitycsca.crt
http://autorite.dhimyotis.com/entitycsca.crt

**FR03**
http://autorite.certigna.fr/2ddoc.crt
http://autorite.dhimyotis.com/2ddoc.crt

**CERTIGNA SERVICES CA**
http://autorite.certigna.fr/servicesca.crt
http://autorite.dhimyotis.com/servicesca.crt

**CERTIGNA WILD CA**
http://autorite.certigna.fr/wildca.crt
http://autorite.dhimyotis.com/wildca.crt

## 12. VÉRIFICATION DES CERTIFICATS

Afin de vérifier la chaîne de certification, l'UTILISATEUR d'un CERTIFICAT peut télécharger les certificats d'autorité (AC RACINE et AC EMETTRICES) depuis le site : https://www.certigna.fr. Le CERTIFICAT d'AUTORITE RACINE peut être déjà installé sur le poste de travail de l'UTILISATEUR suivant la configuration logicielle de ce dernier. Afin de vérifier le statut de REVOCATION d'un CERTIFICAT, l'AC publie de façon périodique la LCR et offre un service d'information sur le statut de révocation des CERTIFICATS (serveur OCSP, pour On-line Certificate Status Protocol). Cette liste des CERTIFICATS révoqués et ces services sont accessibles pour les applications utilisant les CERTIFICATS aux adresses contenues dans les CERTIFICATS.

| | |
|---|---|
| **CERTIGNA IDENTITY CA** | |
| Accès aux LCR | http://crl.certigna.fr/identca.crl<br>http://crl.dhimyotis.com/identca.crl |
| Accès à l'OCSP | http://identca.ocsp.certigna.fr<br>http://identca.ocsp.dhimyotis.com |
| **CERTIGNA IDENTITY PLUS CA** | |
| Accès aux LCR | http://crl.certigna.fr/identityplusca.crl<br>http://crl.dhimyotis.com/identityplusca.crl |
| Accès à l'OCSP | http://identityplusca.ocsp.certigna.fr<br>http://identityplusca.ocsp.dhimyotis.com |
| **CERTIGNA ENTITY CA** | |
| Accès aux LCR | http://crl.certigna.fr/entityca.crl<br>http://crl.dhimyotis.com/entityca.crl |
| Accès à l'OCSP | http://entityca.ocsp.certigna.fr<br>http://entityca.ocsp.dhimyotis.com |
| **CERTIGNA ENTITY CODE SIGNING CA** | |
| Accès aux LCR | http://crl.certigna.fr/entitycsca.crl<br>http://crl.dhimyotis.com/entitycsca.crl |
| Accès à l'OCSP | http://entitycsca.ocsp.certigna.fr<br>http://entitycsca.ocsp.dhimyotis.com |
| **FR03** | |
| Accès aux LCR | http://crl.certigna.fr/2ddoc.crl<br>http://crl.dhimyotis.com/2ddoc.crl |
| Accès à l'OCSP | http://2ddoc.ocsp.certigna.fr<br>http://2ddoc.ocsp.dhimyotis.com |
| **CERTIGNA SERVICES CA** | |
| Accès aux LCR | http://crl.certigna.fr/servicesca.crl<br>http://crl.dhimyotis.com/servicesca.crl |
| Accès à l'OCSP | http://servicesca.ocsp.certigna.fr<br>http://servicesca.ocsp.dhimyotis.com |
| **CERTIGNA WILD CA** | |
| Accès aux LCR | http://crl.certigna.fr/wildca.crl<br>http://crl.dhimyotis.com/wildca.crl |
| Accès à l'OCSP | http://wildca.ocsp.certigna.fr<br>http://wildca.ocsp.dhimyotis.com |

Dans le cadre de l'utilisation du service de répondeur OCSP de CERTIGNA, un nombre maximal de 250.000 requêtes OCSP est autorisé par CERTIFICAT et par jour. En cas de dépassement de ce seuil, CERTIGNA se réserve le droit d'imposer au PORTEUR ou au RC du CERTIFICAT la mise en place du mécanisme d'OCSP Stapling sur le service utilisant le CERTIFICAT. En cas de refus de mise en place de l'OCSP stapling, CERTIGNA pourrait être amenée à révoquer le CERTIFICAT et ce afin de maintenir et garantir la disponibilité du répondeur OCSP pour l'ensemble de ses clients.

## 13. RESPONSABILITÉ ET ASSURANCE

### 13.1. Responsabilité

L'AC est soumise à une obligation générale de moyens. L'AC ne pourra voir sa responsabilité engagée à l'égard du PORTEUR ou du RC que pour les dommages directs qui pourraient lui être imputés au titre des prestations qui lui sont confiées dans le cadre des présentes CGVU.
La responsabilité de l'AC ne pourra pas être recherchée pour tout préjudice indirect, tel que notamment, la perte de chiffre d'affaires, la perte de bénéfice, la perte de commandes, la perte de données, la perte d'une chance, le trouble à l'image ou tout autre dommage spécial ou évènements en dehors de son contrôle ou de tout fait ne lui étant pas imputable.
L'AC n'est responsable que des tâches expressément mises à sa charge dans le cadre du présent CONTRAT.
L'AC ne saurait être tenue responsable de quelque manière que ce soit de l'utilisation faite par le PORTEUR ou le RC du CERTIFICAT, ni du contenu des documents et des données qui lui sont remis par le PORTEUR, le RC ou le demandeur.
En aucun cas, la responsabilité de l'AC ne saurait être recherchée pour :

- Faute, négligence, omission ou défaillance de l'AC, qui constituerait la cause exclusive de survenance du dommage,
- Dysfonctionnement ou d'indisponibilité d'un bien matériel ou immatériel dans le cas où celui-ci a été fourni par le PORTEUR ou le RC,
- Retard dans la fourniture des données à traiter dû au PORTEUR ou RC ;
- Perte de la qualification d'un tiers prestataire qui est indépendant de la volonté de CERTIGNA (Ex : le fournisseur du SUPPORT CRYPTOGRAPHIQUE du CERTIFICAT).

De convention expresse entre les PARTIES, la responsabilité de l'AC est limitée, tous préjudices confondus, à la somme de deux (2) fois le montant réglé au titre du CONTRAT.

**13.2. Assurance**

L'AC est titulaire d'une police d'assurance en matière de Responsabilité Civile Professionnelle, garantissant les dommages directs matériels ou immatériels consécutifs causés dans l'exercice de son activité professionnelle.

## 14. CONTRAT ET MODIFICATIONS

Le CONTRAT annule tout engagement antérieur. Le PORTEUR ou le RC convient que, pendant la durée du CONTRAT, l'AC pourra en modifier les termes unilatéralement et à tout moment. Toutefois, les conditions acceptées et signées par le PORTEUR ou le RC restent valides pendant toute la durée du CONTRAT, sauf si le PORTEUR ou le RC accepte explicitement les nouvelles conditions émises et publiées par l'AC sur le site https://www.certigna.fr ou sur le site de l'AED. La nouvelle version du CONTRAT s'appliquera à toute nouvelle DEMANDE DE CERTIFICAT.

## 15. RÉSILIATION

En cas de manquement par l'une ou l'autre des PARTIES à l'une de ses obligations au titre des présentes, l'autre PARTIE sera autorisée, trente (30) jours après mise en demeure envoyée par lettre recommandée avec avis de réception restée sans effet, à mettre fin aux présentes de plein droit par lettre recommandée avec avis de réception sans préjudice de tous dommages et intérêts auxquels elle pourrait prétendre du fait des manquements invoqués.

## 16. DONNÉES PERSONNELLES

Les dossiers de DEMANDE DE CERTIFICAT comportant les données personnelles sont archivés à minima sept ans et aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable. Les informations personnelles d'identité peuvent être utilisées comme données d'authentification lors d'une éventuelle demande de REVOCATION ou d'informations.
Par ailleurs, CERTIGNA conserve les données à caractère personnel pendant une durée de trois ans à compter de la fin des relations commerciales avec le client et 3 ans à compter du dernier contact émanant avec le prospect. Le délai commence à partir de la dernière connexion au compte client ou du dernier envoi d'un courriel au service client, ou d'un clic sur un lien hypertexte d'un courriel adressé par CERTIGNA, ou d'une réponse positive à un courriel demandant si le client souhaite continuer à recevoir de la prospection commerciale à l'échéance du délai de trois ans.
Afin suivre la qualité de nos services, les appels réalisés auprès de notre service clients sont susceptibles d'être enregistrés et conservés durant une période de trente (30) jours.
Conformément à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et au règlement européen « 2016/679/ UE du 27 Avril 2016 » relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, vous bénéficiez d'un droit d'accès, d'opposition, de rectification, de suppression et de portabilité de vos données personnelles. Vous pouvez exercer votre droit en vous adressant par e-mail à : privacy@certigna.com, ou par courrier à l'adresse suivante :

**CERTIGNA, Service du DPO,**
**20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France**

Votre demande devra indiquer votre nom et prénom, adresse e-mail ou postale, être signée et accompagnée de la copie d'un justificatif d'identité en cours de validité.

## 17. CESSION DU CONTRAT

Le PORTEUR ou le RC ne peut pas céder ses droits liés au CONTRAT.

## 18. REGLEMENT DE CONFLITS

La validité des présentes CGVU et toute autre question ou litiges relatifs à son interprétation, à son exécution ou à sa résiliation seront régis par le droit français.
Les PARTIES s'engagent à consacrer leurs meilleurs efforts à la résolution amiable de toutes les questions ou de tous les litiges qui pourraient les diviser, préalablement à la saisie de la juridiction ci-après désignée.
**Les PARTIES conviennent, pour le cas où un accord amiable serait impossible à arrêter, que les juridictions de Lille auront compétences exclusives pour connaître de tout différend résultant de la validité, de l'interprétation, de l'exécution ou de la résiliation des présentes, et plus généralement de tout litige procédant des présentes qui pourrait les diviser, nonobstant pluralités des défendeurs ou appel en garantie.**

## 19. COORDONNÉES DE LA SOCIÉTÉ CERTIGNA

CERTIGNA S.A.S
Zone de la plaine,
20 allée de la râperie 59650 Villeneuve d'Ascq
Tél : +33 806 115 115
Email : contact@certigna.com

## 20. SIGNALER UN CERTIFICAT MALVEILLANT OU DANGEREUX

Pour signaler un CERTIFICAT malveillant ou dangereux (un CERTIFICAT dont la clé privée est suspectée de compromission, un CERTIFICAT dont l'usage n'est pas respecté, ou tout autre type de fraude : compromission, détournement d'usage, conduite inappropriée, etc.) ou tout autre problème relatif aux CERTIFICATS, veuillez utiliser le formulaire de contact disponible à l'adresse suivante https://www.certigna.fr/contact.xhtml et sélectionner l'objet « Certificat jugé malveillant ou dangereux ».

## 21. PERTE DE QUALIFICATION/CERTIFICATION DU SUPPORT

Le SUPPORT CRYPTOGRAPHIQUE, délivré le cas échéant par CERTIGNA au PORTEUR ou au RC pour stocker et utiliser la clé privée et le CERTIFICAT, bénéficie d'une ou plusieurs qualifications et/ou certifications. Dans le cas où l'une de ces qualifications ou certifications ne serait plus maintenue ou suspendue pour des raisons telles que l'identification d'une vulnérabilité ou l'arrêt de fabrication du produit, CERTIGNA en informera le PORTEUR ou le RC et révoquera son CERTIFICAT, sans condition de remboursement.