CERTIFICATS ÉMIS PAR L'AC « CERTIGNA SERVICES CA »

1. OBJET

Les présentes conditions ont pour objet de préciser les modalités de demande et d'utilisation d'un certificat « Certigna Services CA », proposé à un futur RC et/ou à un RC, ainsi que les engagements et obligations respectifs des parties liées aux présentes. Les conditions générales d'utilisation découlent de la Politique de Certification identifiée par l'OID 1.2.250.1.177.2.5.1 disponible à l'adresse : http://politique.certigna.fr/PCcertignaservicesca.pdf. Les certificats couverts par cette Politique de certification et les présentes conditions ont les OID suivants :

- Certificats d'authentification serveur SSL/TLS * : 1.2.250.1.177.2.5.1.1.1
- Certificats d'authentification de type client * : 1.2.250.1.177.2.5.1.2.1
- Certificats d'authentification serveur qualifié/EV : 1.2.250.1.177.2.5.1.3.1

2. DÉFINITIONS

- **AC** : Autorité de Certification « Certigna Services CA » de la société DHIMYOTIS, délivrant le CERTIFICAT ;
- **AC RACINE** : Autorité de plus haut niveau de l'IGC 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 DHIMYOTIS, contrôlant les demandes de CERTIFICAT et les éventuelles demandes de REVOCATION ;
- **AUTORITE D'ENREGISTREMENT DELEGUEE (AED)** : Entité tierce externe à l'IGC avec laquelle DHIMYOTIS 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 ;
- **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.
- **CONTRAT** : Relations entre l'AC et le RC ;
- **DEMANDE DE CERTIFICAT** : Ensemble constitué du formulaire de demande signé (acceptant les présentes conditions générales d'utilisation) accompagné des pièces justificatives, et de la requête générée informatiquement ;
- **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, éventuellement les attributs des porteurs de cette entité ;
- **OID** : Identifiant d'objet (Object IDentifier) ;
- **OCSP STAPLING** : Configurer le serveur sécurisé du client 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 ;
- **RC** : Personne physique en charge et responsable du CERTIFICAT utilisé pour le SERVEUR et de la clé privée associée ;
- **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 ;
- **UTILISATEUR** : Utilisateur d'un CERTIFICAT. Il peut s'agir de :
  - Pour un CERTIFICAT d'Authentification de type serveur SSL/TLS, 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 serveur de type client, d'un service applicatif accédant à un serveur informatique 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. CONFORMITÉ

LE CERTIFICAT est émis en conformité avec :

- Les exigences de la PC Type « *Certificats électroniques de Services Applicatifs* » pour un usage d'authentification de client/serveur au niveau * du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- Le règlement européen eIDAS et le niveau OCVP / PTC de l'ETSI EN 319 411-1 ;
- Les exigences du document « Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates » du CA/BROWSER FORUM.

4. DURÉE

Le CONTRAT est conclu pour une durée choisie par le futur RC (825 jours maximum) et démarre le jour de la délivrance du CERTIFICAT par l'AE.

5. TARIF

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,
- 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 DHIMYOTIS,
  - espèces pour tout montant n'excédant pas 1000 Euros ;
  - mandat administratif, pour les établissements publics uniquement, en joignant un bon de commande au nom de l'Établissement.
- La REFABRICATION d'un CERTIFICAT logiciel est gratuite durant les 3 mois qui suivent la délivrance du CERTIFICAT par l'AC ;
- Le DEBLOCAGE du SUPPORT CRYPTOGRAPHIQUE dans lequel est fourni le CERTIFICAT est une prestation facturée ;

Sauf accord écrit et préalable de l'AC, 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.441-6 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.

6. OBLIGATIONS DU RC

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 lors de la demande ou du renouvellement du CERTIFICAT ;
- 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, 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 « CERTIGNA SERVICES CA » et qui est pour les certificats RGS * :
  - Soit un dispositif matériel de type carte à puce ou module cryptographique qualifié par l'ANSSI ;
  - Soit une solution logicielle respectant les exigences du chapitre 11.1 de la Politique de Certification via la mise en place de mesures de sécurité additionnelles propres à l'environnement dans lequel est déployé la clé privée. Cet environnement dans lequel est déployée la clé privée doit avoir fait l'objet d'un audit de sécurité.
- Informer l'AE en cas de non réception d'un e-mail confirmant la prise en compte de sa demande de CERTIFICAT ou de REVOCATION.
- Suite à la réception d'un e-mail de l'AE signalant la non-conformité de la demande ou que le dossier est incomplet, d'effectuer les modifications sous 7 jours calendaires après la réception de cet e-mail.
- Télécharger son certificat dans les 30 jours qui suivent la validation de son dossier qui est notifiée par e-mail au RC. Au-delà de ce délai, le CERTIFICAT est révoqué automatiquement par l'AE ;
- Accepter explicitement le CERTIFICAT depuis son espace client CERTIGNA lors de la procédure de téléchargement du CERTIFICAT ou bien par courrier papier signé par 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 du SERVEUR dont il a la responsabilité par des moyens appropriés à son environnement ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du SERVEUR ;
- 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 révocation 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 révocation du chapitre 9 est rencontrée.
- Sauvegarder la clé privée associée au CERTIFICAT. Si elle est stockée sur disque dur, il doit créer, pour sa protection, un mot de passe complexe (c'est-à-dire constitué d'une combinaison de 8 caractères minimum parmi chiffres, lettres minuscules et majuscules, et caractères spéciaux).
- Prendre toutes les mesures propres à s'assurer la sécurité du ou des ordinateurs sur lesquels est installé le CERTIFICAT. 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 révocation 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 RC.
- 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 du CERTIFICAT, qu'elle a émis le CERTIFICAT pour un SERVEUR donné et que le RC correspondant a accepté le CERTIFICAT ;
- Prendre toutes les mesures raisonnables pour s'assurer que 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, notamment par rapport à la CNIL et à l'article 226-13 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002) du Code Pénal.
- 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 pour vérifier que 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).
- Mettre en œuvre et suivre, lors de l'émission d'un certificat, les exigences décrites au chapitre 3.2 et 3.3 de la PC pour vérifier que l'organisation rattachée au serveur a autorisé la délivrance du certificat, et que le RC est autorisé à demande le certificat au nom de l'organisation.
- Mettre en œuvre et suivre, lors de l'émission d'un certificat, les exigences décrites au chapitre 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 au chapitre 3.2 et 3.3 de la PC pour vérifier l'identité de l'organisation, de son représentant et du 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 conditions d'utilisation.
- Mettre à disposition du public 24h/24, 7j/7 les informations sur l'état (valide ou révoqué) des certificats non expirés ;
- Révoquer un certificat pour l'une des raisons spécifiées au chapitre 9.

L'AE s'engage à :

- Vérifier et à valider les dossiers de demande et de révocation de CERTIFICAT ;
- Générer et mettre à la disposition du RC le CERTIFICAT dans un délai de cinq jours ouvrés dans le cas où la demande de CERTIFICAT est conforme et le dossier de demande complet.
- 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 du PORTEUR ne fait pas l'objet de publication.

9. RÉVOCATION

Les principales causes de révocation possibles sont les suivantes :

- Le RC, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- Le représentant légal de l'entité à laquelle il appartient informe l'AC que la demande de certificat originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
- Le RC n'a pas respecté les Conditions Générales d'Utilisation du certificat ou l'AC obtient la preuve que l'usage du certificat est détourné ;
- L'AC est informée que le RC a violé une ou plusieurs de ses obligations en vertu des Conditions Générales d'Utilisation ;
- 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 serveur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple, modification de l'identité ou de la fonction du serveur), ceci avant l'expiration normale du certificat ;
- 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 détecte que les informations apparaissant dans le certificat sont inexactes ou trompeuses ;
- 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 révocation du certificat ;
- Le droit de l'AC pour émettre des certificats sous ces exigences expire ou est révoqué ou est terminé, à moins que l'AC n'ait pris des dispositions pour maintenir la publication des CRL/OCSP ;
- Le certificat de signature de l'AC est révoqué (ce qui entraîne la révocation 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 serveur ou la cessation d'activité de l'entité du RC de rattachement du serveur ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du serveur est suspectée de compromission, est compromise, est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée) ;
- Pour des raisons techniques (échec de l'envoi du certificat, …).

La demande de révocation peut être effectuée par :

- Le RC, un représentant légal de l'entité de rattachement du SERVEUR, ou le cas échéant un MC de cette entité,
- L'AC ou l'AE.

La demande de révocation 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 depuis l'espace client du RC ou du MC le cas échéant.

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

- Pour un CERTIFICAT d'Authentification de type serveur SSL/TLS (qualifié ou non), 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.
- Pour un CERTIFICAT d'Authentification serveur de type client, les usages sont l'authentification du SERVEUR auprès d'autres serveurs, 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.

Le CERTIFICAT est utilisé par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent. En cas de non-respect de ces usages, la responsabilité du RC ou de l'entité à laquelle le SERVEUR est rattachée 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.
- 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 l'AC peut être téléchargé depuis les adresses suivantes :
  - http://autorite.certigna.fr/servicesca.crt ;
  - http://autorite.dhimyotis.com/servicesca.crt.

12. MOYENS OFFERTS POUR LA 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.

Pour accéder à la LCR :
http://crl.certigna.fr/servicesca.crl
http://crl.dhimyotis.com/servicesca.crl

Pour accéder au serveur OCSP :
http://servicesca.ocsp.certigna.fr
http://servicesca.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 RC du CERTIFICAT la mise en place du mécanisme d'OCSP Stapling sur le SERVEUR sécurisé par le CERTIFICAT. En cas de refus de mise en place de l'OCSP stapling, Certigna pourrait être amenée à révoquer le CERTIFICAT du SERVEUR et ce afin de maintenir et garantir la disponibilité du répondeur OCSP pour l'ensemble de ses clients.

13. ÉTENDUE DE RESPONSABILITÉ

La responsabilité de l'AC ne peut être engagée en cas de compromission de la clé privée associée au CERTIFICAT du SERVEUR. L'AC ne sera en aucun cas responsable des éventuels dommages ayant leur origine dans l'utilisation du CERTIFICAT. L'AC ne pourra pas être impliquée par des retards ou pertes que pourraient subir les données échangées avec le SERVEUR et l'authentification du SERVEUR. L'AC ne saurait être tenue responsable de problèmes relevant de la force majeure, au sens du Code civil. Si un cas de force majeure a une durée supérieure à quinze jours, le RC sera autorisé à mettre un terme au CONTRAT et il n'y aura pas de préjudice.

14. CONTRAT ET MODIFICATIONS

Le CONTRAT annule tout engagement antérieur. Le RC convient que, pendant la durée du CONTRAT, l'AC pourra modifier les conditions générales d'utilisation. Toutefois, les conditions acceptées et signées par le RC restent valides pendant toute la durée du CONTRAT, sauf si le RC accepte explicitement les nouvelles conditions émises et publiées par l'AC sur le site https://www.certigna.fr. Un courrier doit dans ce cas être adressé à l'AC en y joignant les nouvelles conditions générales d'utilisation sur lesquelles sont portées la mention "lu et approuvé", la date et la signature du RC. En cas de renouvellement du CONTRAT (renouvellement du CERTIFICAT à la fin de validité de ce dernier ou après sa révocation), le nouveau CERTIFICAT est soumis aux conditions générales d'utilisation en vigueur.

15. RÉSILIATION

Au cas où l'une des parties n'exécuterait pas l'une des obligations découlant des présentes conditions générales, l'autre partie pourra lui notifier d'exécuter ladite obligation. A défaut pour la partie défaillante de s'être exécutée dans les quinze jours de cette notification, l'autre partie pourra résilier le CONTRAT.

16. CONDITIONS DE REMBOURSEMENT

La commande de CERTIFICAT ne peut être annulée dès lors que le dossier est en cours de traitement. Tout CERTIFICAT émis ne peut faire l'objet d'une demande de remboursement.

17. DONNÉES PERSONNELLES

Les dossiers de demande de certificat électronique 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.

Par ailleurs, DHIMYOTIS 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 DHIMYOTIS, 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.

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 mail à : privacy@certigna.com, ou par courrier à l'adresse suivante : DHIMYOTIS, Service du DPO, 20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France.

18. CESSION DU CONTRAT

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

19. REGLEMENT DE CONFLITS

Le CONTRAT est soumis au droit français.

Les parties s'engagent à tenter de résoudre à l'amiable tout différend susceptible d'intervenir entre elles, soit directement soit via un médiateur, dans les 2 mois de la réception du courrier avec accusé réception informant du différend. Les éventuels frais de médiation seront supportés par moitié par chacune des parties. Le cas échéant, l'affaire sera portée devant le tribunal de commerce de Lille.

20. COORDONNÉES DE LA SOCIÉTÉ DHIMYOTIS

Dhimyotis S.A.
Zone de la plaine,
20 allée de la râperie 59650 Villeneuve d'Ascq
Tél : +33 320 792 409 - Fax : +33 956 952 412
Email : contact@dhimyotis.com

21. 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 ».