



## 1. Objet

Les présentes Conditions Générales d'Utilisation (CGU) ont pour objet de définir les conditions juridiques, organisationnelles, techniques et financières relatives à l'obtention des Certificats SSL RGS 1 étoile de Keynectis par le Client ainsi que les conditions d'utilisation et les obligations respectives des Parties.

**La demande de Certificat SSL RGS 1 étoile sur le site web de Keynectis par le Client (ci-après la « Commande ») sera considérée comme étant l'acceptation inconditionnelle et irrévocable du Client d'adhérer aux présentes CGU, et comme une renonciation à ses propres conditions générales d'achat.**

Aucune Commande ne pourra être annulée ou modifiée par le Client, sans l'accord préalable écrit de Keynectis.

## 2. Définitions

**Autorité de Certification (ou AC) :** désigne l'un des acteurs de l'Infrastructure de Gestion de Clés (IGC) générant et distribuant des Certificats SSL qualifiés RGS \*, et ce en application des règles déterminées dans la Politique de Certification (PC) dont l'OID est 1.3.6.1.4.1.22234.2.5.3.6 et les pratiques déterminées dans la Déclaration des Pratiques de Certification (DPC) associée. Dans le cadre des présentes, l'Autorité de Certification émettrice des Certificats dénommée « Keynectis SSL RGS » est signée par l'ACR Class 2 Primary CA.

**Autorité d'Enregistrement (ou AE) :** désigne l'un des acteurs de l'IGC, reconnue par l'AC, pour procéder à l'authentification et à la vérification de l'identité des demandeurs de certificats SSL 1 étoile, conformément aux procédures définies dans la Politique de Certification établie par l'AC. Dans le cadre des présentes, l'AE désigne le service-clients de KEYNECTIS.

**Certificat(s) KWA :** désigne(nt) les Certificats générés à la volée par l'AC de KEYNECTIS pour le compte de la personne qui s'authentifie suivant un login/mot de passe fourni par l'AE de KEYNECTIS et un protocole de consentement, et dont la clé privée associée est utilisée pour la signature électronique de formulaire de demande de certificats via le Portail web de signature.

**Certificat SSL 1 étoile ou Certificat :** désigne un certificat électronique ayant pour objet de permettre la mise en place d'une connexion SSL « Secure Socket Layer » sécurisée entre un serveur de site web disposant du Certificat SSL 1 étoile et l'Utilisateur de Certificat se connectant au site web (key usages : digital signature). Le Certificat est associé à un service d'horodatage et d'OSCP.

**Client :** désigne toute personne, entreprise ou entité qui réalise auprès de Keynectis une demande de Certificat SSL pour sécuriser son site Web dans le cadre de son activité professionnelle et qui contracte avec Keynectis.

**Code de révocation :** désigne le code adressé par KEYNECTIS au Client par courrier électronique lui permettant de révoquer seul son Certificat SSL 1 étoile sur l'URL de révocation.

**Contact Technique :** Un Contact Technique est une personne nommée et autorisée par le propriétaire du nom de domaine à :

- Agir en tant que demandeur SSL pour la génération de la CSR ;

- Générer les bi-clés dont les clés publiques seront associées à un certificat SSL ;
- Remplir les formulaires de demande de certificat SSL ;
- Retirer les certificats SSL ;
- Procéder le cas échéant aux demandes de révocation des certificats SSL.

Dans la terminologie du RGS, le CT est un RCAS (Responsable du certificat d'authentification serveur).

**Contrat :** désigne l'ensemble contractuel constitué par ordre de priorité décroissant : (i) des présentes Conditions Générales d'Utilisation, (ii) du formulaire de demande de Certificat, (iii) des procédures applicables accessibles sur le site web de Keynectis, incluant la Politique de Certification.

**Demande de certificat :** désigne l'ensemble des formulaires (demande d'émission ou de renouvellement de certificat,) dument complétés et signés (de manière manuscrite ou électronique), ainsi que les pièces justificatives associées (telles que la pièce d'identité officielle) transmis par le Contact Technique à l'AE soit par courrier postal soit en utilisant la procédure dématérialisée de KEYNECTIS (via le portail web de signature K.Websign@).

**FQDN ou Fully Qualified Domain Name (ou nom de domaine complètement qualifié) :** désigne un nom de domaine qui indique la position absolue d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine. On parle également de domaine absolu, par opposition aux domaines relatifs.

**Infrastructure de Gestion de Clés (ou IGC) :** désigne un ensemble de moyens techniques, humains, documentaires et contractuels destinés à assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'IGC génère, distribue, gère et archive les Certificats ainsi que les listes de certificats révoqués (LCR) et génère et distribue les Supports.

**Liste des Certificats Révoqués (ou LCR) :** désigne la liste des Certificats non valides et révoqués avant leur date d'échéance, émise périodiquement et numériquement signée par l'AC émettrice des Certificats contenus dans la liste.

**Nom de domaine :** désigne l'identifiant du site web à sécuriser, tel qu'indiqué dans la Commande du Client, et enregistré auprès d'un Office d'enregistrement. Il est constitué de plusieurs éléments : (i) la racine qui est en principe le nom de l'entreprise ou de l'activité ; (ii) une extension ou suffixe séparée de la racine par un point. L'ensemble accolé forme le nom de domaine.

Le nom de domaine doit toujours être enregistré au nom de l'organisation qui en fait la demande. Pendant le processus d'enregistrement, le nom de domaine est « associé » à un Contact Technique qui est juridiquement autorisé à utiliser ce nom de domaine.

**Politique de Certification :** désigne l'ensemble de règles identifiées par un OID et publiées par l'AC décrivant les caractéristiques générales des Certificats qu'elle délivre. Ce document décrit également les obligations et responsabilités de l'AC, de l'AE, du Client, des Utilisateurs de Certificats et de toutes les composantes de l'IGC intervenant dans l'ensemble du cycle de vie d'un Certificat SSL 1 étoile. Dans le cadre des présentes, le Client devra respecter les règles décrites dans la Politique de Certification (PC) dont l'OID est 1.3.6.1.4.1.22234.2.5.3.6, applicable et consultable à l'adresse web suivante : <http://www.keynectis.com/PC>.



**Portail web de signature** : désigne l'interface web par laquelle le Client accède en s'authentifiant à l'aide d'un login et d'un mot de passe pour signer électroniquement des Formulaires nécessaires à l'obtention de Certificats SSL 1 étoile, au moyen d'une Clé privée associée à un Certificat KWA généré suite à la saisie par le Client d'un mot de passe qu'il a préalablement reçu par SMS au numéro de téléphone indiqué sur le Formulaire ou par courrier électronique à l'adresse électronique indiquée sur le Formulaire et ce, suivant le Protocole de consentement figurant sur le Portail web de signature. Le Portail envoie, par courrier électronique, le Formulaire signé à l'AE pour vérification. Le Portail web de signature permet ainsi de signer électroniquement, via l'application K.Websign®, des Formulaires et de les conserver en leur conférant la même valeur légale qu'un écrit sur support papier, en conformité avec les dispositions des articles 1316-1 et de la première phrase du second alinéa de l'article 1316-4 du Code civil. Il est précisé que le Portail web de signature ne permet de signer électroniquement que des Formulaires signés par Keynectis. Tout autre document sera rejeté et ne sera pas signé.

**Propriétaire du Nom de Domaine** : désigne l'entité légale qui détient le nom de domaine concerné par la délivrance d'un Certificat SSL 1 étoile. Le nom de domaine est géré par un administrateur de nom de domaine. Le propriétaire de nom de domaine fait appel à un Contact Technique ou un Administrateur SSL pour gérer les certificats SSL associé aux noms de domaines dont il est propriétaire.

**Protocole de consentement** : désigne une rubrique du Formulaire de demande de Certificat SSL 1 étoile par laquelle le Client atteste sur l'honneur de l'exactitude et la véracité des informations qu'il a fournies, de son engagement de signature, et de l'acceptation sans réserve des présentes CGU de KEYNECTIS.

**Révocation (d'un Certificat)** : désigne l'opération demandée par le Client, l'AC ou l'AE conformément à la Politique de Certification, dont le résultat consiste en la suppression de la garantie de l'AC sur un Certificat donné, avant la fin de sa période de validité.

**Signature électronique** : désigne, aux termes de l'article 1316-4 du Code civil, « l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache » et a pour objet d'identifier la personne qui l'appose et de manifester le consentement de la personne aux obligations qui découlent de l'acte signé.

**Utilisateur de Certificat** : désigne une personne ou une machine qui fait confiance aux certificats SSL 1 étoile, fait confiance au chemin de certification de l'AC, afin d'identifier et d'authentifier un Nom de domaine et l'entité dont le nom de domaine est inclus dans le Certificat SSL 1 étoile.

### **3. Description du service de certification SSL**

Les conditions d'utilisation du service de certification électronique de KEYNECTIS sont décrites et régies par la Politique de Certification de l'Autorité de Certification de KEYNECTIS, laquelle fait partie intégrante des présentes. La Politique de Certification et ses versions successives sont publiées sur le site Internet de KEYNECTIS à l'adresse suivante : <http://www.keynectis.com/PC>. En acceptant les présentes conditions générales, le Client reconnaît avoir pris connaissance et être lié par les termes de la Politique de

Certification applicable à la date de Commande et ses mises à jour successives.

### **4. Traitement des demandes d'émission de Certificat SSL**

Le Contact Technique effectue une Demande de Certificat selon la procédure indiquée dans la Politique de Certification, auprès de l'AE, soit en version papier, soit sous forme électronique en utilisant le portail web de signature de KEYNECTIS.

Les modalités pratiques d'élaboration d'une Demande de Certificat sont transmises par l'AE de KEYNECTIS.

Dans tous les cas, toute Demande de Certificat (papier ou électronique) doit être signée par le Client.

La signature manuscrite ou électronique répond à la définition donnée par la première phrase du second alinéa de l'article 1316-4 du Code civil issu de la Loi n°20 00-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

A réception de la demande d'un Certificat SSL effectuée par un Client, l'AE procède à la vérification des informations et pièces fournies par le Client.

En outre, l'AE vérifie la bonne réception de la Commande et de son complet paiement.

Lors de la demande, le Client s'engage à fournir toutes informations utiles, exactes et complètes lors de la création ou du renouvellement du Certificat.

Toute modification d'information signalée comme obligatoire doit être notifiée par écrit à KEYNECTIS et accompagnée de justificatifs requis.

En tout état de cause, le Client est informé qu'en cas de dossier incomplet, ou dans l'hypothèse où le Client n'aurait pas communiqué à Keynectis les informations nécessaires demandées, KEYNECTIS en informe le Client. La demande de Certificat SSL sera alors mise en attente par KEYNECTIS jusqu'à complétude du dossier.

En tout état de cause, le Certificat SSL ne sera délivré au Client qu'à réception du complet paiement de la Commande.

Après avoir récupéré et installé son Certificat, le Client devra en contrôler le contenu et informer KEYNECTIS de toute erreur qu'il aurait détectée. Dans ce cas, KEYNECTIS révoquera ledit Certificat et émettra un nouveau Certificat corrigé.

### **5. Accès au Portail web de signature**

Le Portail web de signature est accessible par le Client par le biais d'une connexion à distance au moyen d'un login et d'un mot de passe.

A cet égard, Keynectis ne saurait être responsable des conséquences dommageables qui pourraient résulter de l'utilisation du Portail web de signature par un tiers non autorisé, suite à une faute ou négligence du Client dans la sécurité de ses login/mot de passe.

Par ailleurs, Keynectis adressera au numéro de téléphone ou à l'adresse de courrier électronique communiqué par le Client sur le Formulaire électronique de Demande de Certificat un mot de passe qui, lors de sa saisie par le Client via le Portail web de signature, génèrera une bi-clé et un Certificat KWA lui permettant de signer ledit Formulaire.

A ce titre, Keynectis n'est aucunement responsable de :



- la signature électronique du Formulaire par un tiers non autorisé, résultant de la divulgation, directe ou indirecte, volontaire ou involontaire, par le Client de son mot de passe ;
- la perte ou vol du téléphone sur lequel le Client a reçu le SMS, ou la destruction par le Client du SMS ou du courrier électronique communiquant ledit mot de passe ;
- l'identification et l'authentification du Client sur le Portail web de signature ;
- la perte de son Code de révocation ou la destruction du courrier électronique le contenant.

Par ailleurs, le Client est seul responsable de la sécurité physique et logique concernant l'accès au Portail web de signature ainsi que de toutes les conséquences et actions qui résulteraient d'une utilisation non autorisée dudit Portail.

Par « accès au Service K.Sign\*\* », il faut entendre l'accès à toutes informations et tous moyens permettant de réaliser une Demande de Certificats et qui déclenche, en cas d'authentification réussie de la part de l'AE, une mise en œuvre du service de certification SSL.

En tout état de cause, le Client s'engage à informer immédiatement Keynectis et par écrit de toute utilisation détournée ou non autorisée du Portail web de signature dont elle aurait connaissance, et de toute atteinte à la sécurité pouvant en résulter.

En conséquence, et de convention expresse, les Parties conviennent que Keynectis ne saurait être tenue responsable de tout dommage résultant de l'utilisation du Service par un tiers non autorisé qu'il s'agisse de l'un des salariés, agents, sous-traitants, fournisseurs, prestataires de services du Client.

Par ailleurs, le Client déclare accepter les caractéristiques et les limites d'Internet, et en particulier reconnaît :

- Avoir connaissance de la nature d'Internet et en particulier des limites quant à ses performances techniques et les temps de réponse pour consulter, interroger ou transférer des informations ;
- Que la communication éventuelle par Internet de mots de passe, codes confidentiels et d'une manière générale, toute information confidentielle est faite à ses risques et périls ;
- Que les données circulant sur Internet pouvant être réglementées en termes d'usage ou être protégées par un droit de propriété, elle est seule responsable de l'usage des données qu'elle consulte, interroge et transfère sur Internet ;
- Qu'elle doit prendre toutes les mesures appropriées de façon à protéger ses propres systèmes informatiques des intrusions non autorisées, des actes de destruction ou d'altération, des contaminations éventuelles par des virus, chevaux de Troie ou autre système causant des failles de sécurité sur Internet.

## **6. Durée de vie d'un certificat SSL**

Le Certificat SSL 1 étoile a une durée de validité de un (1), deux (2) ou trois (3) ans selon l'option choisie par le Client. Cette durée débute à compter de sa date d'émission par l'Autorité de Certification.

## **7. Renouvellement d'un Certificat SSL**

Le renouvellement d'un Certificat SSL 1 étoile implique la génération d'un nouveau Certificat, et se fait suivant la même procédure qu'une demande initiale de Certificat.

## **8. Révocation d'un Certificat SSL**

La Révocation du Certificat par le Client peut être faite :

- Soit depuis le site web de Keynectis à l'aide son code de révocation (fourni par KEYNECTIS). KEYNECTIS génère et transmet ce code de révocation au Client, par courrier électronique lors de la remise du code PIN et du support;
- Soit sur demande faite auprès de l'AE de KEYNECTIS (service-clients).

Le Certificat SSL 1 étoile peut être révoqué lorsque le lien entre ce dernier et la clé publique associée n'est plus valable. Le Client devra avertir sans délai KEYNECTIS et faire une demande en ligne de révocation du Certificat dans les cas suivants :

- compromission avérée ou soupçonnée de la sécurité de sa clé privée ;
- détection d'une erreur d'une information contenue dans le Certificat ;
- changement d'une information contenue dans le Certificat ;
- changement du nom de domaine ou du nom de l'organisation enregistré.

La demande de révocation par le Client est soumise à une procédure identique à celle relative à l'émission d'un Certificat SSL.

Keynectis se réserve le droit de révoquer le Certificat avec effet immédiat et sans préavis dans le cas où elle découvre que les informations contenues dans le Certificat ne sont plus valides.

Le Certificat révoqué sera inscrit dans la LCR au plus tard dans les vingt-quatre (24) heures suivant sa révocation.

## **9. Durée du Contrat**

Le présent Contrat prend effet à la date de commande du Certificat SSL 1 étoile par le Client et il a pour terme la date de fin de validité du certificat commandé et émis.

En cas de manquement par l'une des Parties à l'une de ses obligations contractuelles, non remédié dans le délai de 30 jours francs à compter de la réception d'une lettre recommandée avec avis de réception identifiant avec précision le manquement en question et demandant d'y remédier, la résiliation sera effective de plein droit. Cette résiliation interviendra sans préjudice de toute demande de dommages et intérêts auxquels la partie non défaillante pourrait avoir droit. En cas de résiliation pour manquement du Client consistant en un défaut de sécurité qui lui serait imputable, KEYNECTIS se réserve le droit de révoquer sans délai son certificat SSL 1 étoile.

## **10. Conditions financières**

Le prix du Certificat SSL applicable est celui mentionné dans l'offre en ligne de KEYNECTIS à la date de souscription ou du renouvellement dudit certificat SSL. Les conditions tarifaires du Certificat SSL dépendent de leur durée de validité et du type de Certificat choisi par le Client.

A l'issue de la réception par Keynectis de la demande de Certificat par le Client, une facture sera adressée par courriel au Client. La facture est payable en ligne par carte bancaire ou par virement ou chèque. A réception du paiement du Client, KEYNECTIS procèdera à la délivrance du Certificat. En cas de dossier d'inscription incomplet rendant impossible la délivrance du Certificat commandé, KEYNECTIS se



réserve le droit de conserver le montant payé par le Client au moment de la commande. Pour les cas de demande d'annulation de la Commande notifiée à Keynectis par lettre recommandée avec AR dans un délai d'un mois à compter de la date de commande, l'intégralité du montant versé restera acquis à Keynectis à titre d'astreinte.

## 11. Restrictions d'usage

Le Client s'engage à n'utiliser les Certificats qui lui sont délivrés qu'en son nom propre.

Ainsi, il lui est interdit d'utiliser le Certificat pour le compte d'autres organisations, ou pour réaliser des opérations de clé privée ou publique en rapport avec un nom de domaine ou un nom d'organisation autre que celui qu'il a déclaré dans sa demande de certificat.

Le Client s'engage à ne télécharger le Certificat que sur un seul poste informatique.

Il s'interdit d'utiliser le Certificat et sa clé privée associée sur un nombre de serveurs ou de dispositifs physiques supérieur au nombre de licences souscrites.

En outre, le Client est informé que l'utilisation sans licence d'un Certificat SSL sur un serveur ou un dispositif résidant sur un serveur constitue un acte de piratage et engagera des poursuites à l'encontre des contrevenants dans les limites autorisées par la loi.

## 12. Engagements du Client

Le Client s'engage à suivre les étapes de demande de Certificat sur le site web de Keynectis et à transmettre à Keynectis toutes les informations nécessaires pour le traitement de la Commande et l'émission du Certificat.

Le Client s'engage à ce que (i) les informations transmises pour l'émission du Certificat soient exactes, (ii) qu'elles ne constituent pas une violation des droits de propriété intellectuelle d'un tiers, (iii) qu'elles n'ont pas été ou ne seront pas utilisées à des fins illégales.

Le Client s'engage à utiliser le Certificat SSL et les autres services d'émission, de renouvellement et de révocation que l'Autorité de Certification délivre conformément aux dispositions de la Politique de Certification et aux présentes.

Le Client s'engage à prendre toutes les mesures propres à assurer la sécurité du serveur où est installé le Certificat et à prendre toutes dispositions nécessaires à la sauvegarde sécurisée du Certificat.

En outre, le Client s'engage à conserver et protéger en confidentialité et en intégrité sa clé privée et à ne pas la divulguer sous quelle que forme que ce soit. Il garantit rester la seule personne en possession de sa clé privée, de son mot de passe et identifiant personnel, de tout dispositif logiciel ou matériel protégeant sa clé privée, et qu'aucune personne non autorisée n'a eu, ou n'aura accès à ces éléments.

A cet égard, il supportera seul les conséquences dommageables qui pourraient résulter de l'utilisation par un tiers qui aurait eu communication, par quel que moyen que ce soit, de la Clé privée et de son Certificat.

Au cas où le Nom de domaine enregistré dans le Certificat ou l'organisation du Client changerait, le Client doit sans délai procéder à une demande de révocation en ligne de son Certificat. Le Client s'engage dans ce contexte à ne plus utiliser le Certificat concerné.

Suite à l'expiration ou à la notification de la révocation du Certificat, le Client s'engage à définitivement retirer le Certificat du serveur sur lequel il est installé et ne doit plus utiliser ce Certificat quelle qu'en soit la raison.

## 13. Engagements de Keynectis

KEYNECTIS est tenue à une obligation de moyens pour toutes les obligations relatives à la gestion de vie des Certificats SSL qu'elle émet.

Elle met à la disposition du Client une interface web d'enregistrement des demandes.

Elle se réserve le droit de suspendre l'accès au site lorsqu'elle estime qu'un événement susceptible d'en affecter le fonctionnement ou l'intégrité le nécessite, et ce pour la durée nécessaire à l'intervention envisagée.

Keynectis s'engage à mettre à disposition du Client un service-clients qui, en qualité d'AE, traitera les questions relatives aux demandes d'émission, de renouvellement et de révocation de Certificat SSL. Les horaires d'ouverture du service clients de KEYNECTIS sont du lundi au vendredi, de 9h à 18h, heure française, jours ouvrés. Le service clients de KEYNECTIS est accessible par email ou par téléphone.

## 14. Responsabilité

### 14.1 Responsabilité du Client

Le Client reconnaît avoir pris connaissance et accepter les exclusions et limitations de garanties contenues dans les présentes et la Politique de Certification.

Le Client est seul responsable de la génération, de la conservation et de la protection de sa clé privée.

Par ailleurs, il garantit KEYNECTIS contre toute réclamation ou action, d'un tiers invoquant :

- un manquement à l'un de ses engagements contractuels, notamment spécifiés à l'article 12 ci-avant ;
- de toute déclaration mensongère ou fausse information donnée dans sa demande de Certificat ;
- de toute violation des droits de propriété intellectuelle de toute personne physique ou morale tierce sur des informations ou contenus qu'il a fournis à KEYNECTIS ;
- de l'impossibilité de publier certains éléments de sa demande de certificat du fait de fausses informations ou d'omission résultant d'une négligence ou de l'intention de nuire à un tiers ;
- de l'impossibilité pour lui de protéger sa clé privée ou de prendre les mesures nécessaires pour prévenir la compromission, la perte, l'altération ou l'utilisation non autorisée de sa clé privée.

A cet égard, le client prendra à sa charge toutes les conséquences financières qui découlent d'une telle action, notamment les dommages intérêts et les dépens.

### 14.2 Responsabilité de KEYNECTIS

KEYNECTIS n'est pas responsable quant à la forme, la suffisance, l'exactitude, l'authenticité la falsification ou l'effet juridique des documents et informations remis lors d'une demande d'émission, de renouvellement ou de révocation d'un Certificat.

KEYNECTIS ne garantit pas l'exactitude des informations fournies par le Client à l'Utilisateur de Certificat, ni les conséquences d'une négligence ou d'un manque de précaution ou de sécurité imputable au Client.

En outre, le Client demeure responsable à l'égard de KEYNECTIS de toute utilisation non autorisée du Certificat et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée.

KEYNECTIS n'assume aucun engagement ni responsabilité quant aux conséquences dues à tout retards, perte, altération, destruction, utilisation frauduleuse des données, transmission accidentelle de virus ou tout autre élément nuisible via toute télécommunication telle que Internet. En



outre, KEYNECTIS n'est pas responsable de la qualité de la liaison internet du Client.

Dans le cas où la responsabilité de KEYNECTIS serait retenue au titre des présentes Conditions Générales d'Utilisation, il est expressément convenu que KEYNECTIS serait tenue à réparation des dommages directs certains et immédiats, dont le Client apportera la preuve, dans la limite de cinquante mille euros (50 000 €), tous faits générateurs confondus.

En outre, Keynectis exclut toute responsabilité en cas de non respect par le Client de ses obligations définies dans les présentes et dans la Politique de Certification.

KEYNECTIS ne sera pas responsable des préjudices indirects et/ou imprévisibles subis par le Client, tels que notamment les pertes de bénéfices, de vente, de contrats, de chiffre d'affaires, de revenus ou d'économies anticipées, perte de clientèle, préjudice d'exploitation, perte de données ou usage de celles-ci, inexactitude ou corruption de fichiers, en relation ou provenant de l'inexécution ou exécution fautive des présentes ou inhérents à l'utilisation des Certificats émis par KEYNECTIS.

Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure au sens de l'article 15 ci-après.

#### **15. Force majeure**

Le Client est informé que la survenance d'un cas de force majeure ou d'un cas fortuit suspendra l'exécution des obligations de KEYNECTIS telles que définies aux présentes, sans que la responsabilité de KEYNECTIS puisse être recherché de ce fait. La force majeure ou le cas fortuit s'entendent de tout événement extérieur à l'une des Parties, tel que définie par la jurisprudence des tribunaux français et par l'article 1148 du Code civil, y compris les grèves totales ou partielles, internes ou externes à l'entreprise, intempéries, épidémies, blocages des moyens de transport ou d'approvisionnement, pour quelque raison que ce soit, tremblement de terre, incendie, tempête, inondation, dégâts des eaux, restrictions gouvernementales ou légales, modifications légales ou réglementaires des formes de commercialisation, virus, pannes d'ordinateurs, blocage des télécommunications, tout incident survenant sur le réseau d'un opérateur tiers, les conflits sociaux autres que ceux impliquant directement l'une des Parties, pannes d'électricité, défaillance du système informatique des Parties ou de tiers, du réseau ou des installations ou réseaux de télécommunications.

#### **16. Propriété intellectuelle**

KEYNECTIS conserve tous les droits de propriété intellectuelle sur ses produits, logiciels, services, concepts, techniques, inventions, procédés, savoir-faire, travaux qu'il a développés, intégrés, ou utilisés dans le service SSL qu'il fournit au titre des présentes, et notamment tous les travaux dérivés, modifications, améliorations, configurations, traductions, mises à jour et interfaces.

En conséquence, aucun droit de propriété ou de licence n'est transféré au Client sur ces éléments.

#### **17. Protection des données à caractère personnel**

Chacune des Parties prendra toutes les mesures adéquates en matière de protection des données à caractère personnel et se conformera pour l'exécution des présentes, aux obligations découlant des textes nationaux européens et le

cas échéant internationaux en matière de protection des données personnelles. Chacune des Parties veillera à se conformer aux dispositions légales en vigueur relatives à la protection des données personnelles et notamment à la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004, et procédera ou fera procéder aux formalités nécessaires.

Le Client veillera à déclarer Keynectis comme sous-traitant ayant accès aux informations à caractère personnel ainsi traitées.

En outre, le contact du Client ayant le pouvoir d'accomplir tout acte nécessaire à l'exécution des présentes CGU (notamment les demandes de certificats) au nom du Client dispose sur ses données personnelles d'un droit d'accès, de rectification, et de suppression qu'il peut exercer en s'adressant au Correspondant Informatique et Liberté de KEYNECTIS à l'adresse e-mail suivante : sandrine.barilli@keynectis.com

#### **18. Confidentialité**

Chaque Partie s'engage à conserver confidentielles toutes les informations fournies dans le cadre des présentes par l'autre Partie, sous quelque forme que ce soit (papier, dessin, supports informatiques, etc.), par oral ou par écrit, et incluant sans limitation, toute information technique, commerciale, stratégique, juridique, marketing et/ou financière, toute information sur le savoir-faire, tous brevets, toutes marques, tous dessins, tous modèles, toutes définitions, toutes spécifications, et à ne pas les divulguer à des tiers pendant toute la durée des présentes ainsi que pendant une période de cinq (5) années suivant l'expiration ou la résiliation de celui-ci. De même, constituent des Informations Confidentielles les clés privées du Client, les login/mots de passe d'accès au Portail web de signature, les secrets de l'IGC, les journaux d'évènements des composants de l'IGC, les dossiers d'enregistrement des Clients, et les causes de révocations des Certificats.

En outre, le Client, est tenu d'appliquer des procédures de sécurité pour garantir la confidentialité de ces informations.

#### **19. Dispositions diverses**

##### **19.1 Communication**

Le Client autorise KEYNECTIS à citer, à titre de référence commerciale, son nom, son logo ainsi que sa marque, dans toute documentation commerciale, marketing, y compris sur son site Internet et à reproduire, sur tous types de support tout signe distinctif dont il est titulaire et lui concède à cet effet une licence d'utilisation sur lesdits signes pour les besoins et la durée des présentes.

##### **19.2 Cession du contrat**

Les Parties s'interdisent de céder le Contrat ainsi que les droits et obligations pris séparément sans l'accord exprès et préalable de l'autre Partie.

En cas de changement de contrôle ou de propriété affectant KEYNECTIS au cours de l'exécution du Contrat, résultant d'une fusion, scission, apport partiel d'actif, ou toute autre opération de transmission universelle de son patrimoine, les droits et obligations de Keynectis découlant dudit Contrat seront transmis automatiquement au successeur sans qu'il soit nécessaire pour Keynectis de recueillir l'accord de la part du Client.

##### **19.3 Assurance**

Keynectis atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations relatives au présent Contrat.

##### **19.4 Convention de preuve**



Conformément à l'article 1316-2 du code civil, les Parties entendent fixer, dans le cadre du Contrat, les règles relatives aux preuves recevables entre elles en cas de litige. Les dispositions qui suivent constituent ainsi la convention de preuve passée entre les parties, lesquelles s'engagent à respecter le présent article.

Dans le cadre des échanges entre les parties, la date de réception du message par le destinataire et la signature de ce message valent preuve entre elles et justifient que la notification est imputable à la partie émettrice dudit message. Les Parties s'engagent à accepter qu'en cas de litige les éléments d'identification, les Certificats utilisés sont admissibles devant les tribunaux et feront preuve des données et des faits qu'ils contiennent ainsi que des signatures et procédés d'authentification qu'ils expriment.

Les Parties s'engagent à accepter qu'en cas de litige, les courriels et documents électroniques échangés entre elles sont admissibles devant les tribunaux et font preuve des données et des faits qu'ils contiennent.

Dans le cadre de la relation entre les Parties, la preuve des connexions et d'autres éléments d'identification sera établie autant que de besoin à l'appui des journaux de connexion tenus à jour par les Parties.

#### 19.5 Invalidité d'une clause - Nullité

Si une ou plusieurs stipulations des présentes sont tenues pour non valides ou déclarées telles en application d'une loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations conserveront leur pleine validité sauf si elles présentent un caractère indissociable avec la stipulation non valide.

La nullité d'une clause quelconque des présentes n'affecte pas la validité des autres clauses ; il se poursuit en l'absence du dispositif annulé sauf si la clause annulée rend la poursuite du Contrat impossible ou déséquilibrée par rapport aux conventions initiales.

#### 19.6 Notifications

Toute notification adressée au titre du Contrat sera envoyée par lettre recommandée avec avis de réception adressée au siège social des Parties. Toute réclamation du Client devra, sous peine de forclusion, être adressée par lettre recommandée avec accusé de réception à la personne signataire du Contrat dans un délai de un (1) mois suivant la survenance de l'événement motivant ladite réclamation.

#### 20. Attribution de juridiction – Loi applicable

La loi applicable aux présentes est le droit français.

En cas de litige sur leur interprétation ou leur exécution, pour le cas où les parties ne parviendraient pas à trouver un accord amiable dans un délai de 30 jours sauf à ce que ce délai soit reconduit expressément entre les Parties, il est attribué compétence expresse et exclusive au Tribunal de Commerce de Paris, lequel sera la seule Juridiction compétente pour connaître de tout différend, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires par voie de référé ou requête ou les oppositions sur injonction de payer.

**NOM DU SIGNATAIRE**  
**SIGNATURE**

