Contrat de Souscription GlobalSign - Version 3.8
Le présent document est une traduction de la version originale en anglais hébergée à l'adresse www.globalsign.com/en/repository. En cas de divergence entre les interprétations d'une version traduite et de la version originale en anglais, cette dernière prévaudra.

MERCI DE LIRE ATTENTIVEMENT LE PRESENT CONTRAT AVANT D'UTILISER LE CERTIFICAT DELIVRE A VOTRE ORGANISATION OU A VOUS-MEME. EN DEMANDANT UN CERTIFICAT, VOUS ACCEPTEZ D'ETRE LIE PAR LES TERMES DU PRESENT CONTRAT. SI VOUS N'ACCEPTEZ PAS LES CONDITIONS DU PRESENT CONTRAT, ANNULEZ VOTRE COMMANDE DANS UN DELAI DE SEPT (7) JOURS A COMPTER DE LA DISPONIBILITE DU CERTIFICAT AFIN D'OBTENIR UN REMBOURSEMENT INTEGRAL. SI VOUS AVEZ DES DIFFICULTES POUR COMPRENDRE LE PRESENT CONTRAT, ENVOYEZ-NOUS UN EMAIL A legal@globalsign.com

Le présent Contrat de Souscription GlobalSign (ci-après le « Contrat ») entre GlobalSign et le Demandeur ou le Souscripteur prend effet à compter de la date de demande de Certificat (ci-après la « Date de prise d'effet »).

1.0 Définitions et incorporation par renvoi

Les définitions suivantes sont utilisées dans le présent Contrat :

Affilié : société, partenariat, co-entreprise ou autre entité qui contrôle une autre entité ou une agence, un service, une subdivision administrative ou toute entité opérationnelle sous le contrôle direct d'une Institution Publique, qui est contrôlée par lui/elle ou qui est sous un contrôle commun avec lui/elle.
Demandeur : personne Morale ou physique qui fait une demande de Certificat Électronique (ou en sollicite le renouvellement). Lorsque le Certificat Électronique est émis, il est fait référence à la Personne Morale comme le Souscripteur. Pour les Certificats Électroniques délivrés à des appareils, le Demandeur est l'entité qui contrôle ou exploite l'appareil désigné dans le Certificat Électronique, même si c'est l'appareil qui envoie la Demande de Certificat Électronique effective.
Fournisseur d'Applications Logicielles : fournisseur de logiciels de navigation sur Internet ou d'autres applications logicielles de Parties Utilisatrices, qui utilise ou affiche des Certificats et intègre des Certificats Racine.
Accès à l'Information sur l'Autorité : extension du Certificat indiquant comment accéder aux informations et services de l'émetteur du Certificat Électronique dans lequel elle figure.
CA/Browser Forum : groupe d'experts regroupant des Autorités de certification et des Fournisseurs d'Applications Logicielles. Pour plus d'informations à ce sujet, merci de vous rendre sur www.cabforum.org.
Certificat : document électronique comprenant une Signature Électronique qui lie une Clé Publique à une identité.
Bénéficiaires du Certificat : le Souscripteur, qui est une partie au Contrat de Souscription ou aux Conditions d'Utilisation du Certificat, tous les Fournisseurs d'Applications Logicielles avec lesquels GlobalSign a conclu un contrat d'intégration de son Certificat Racine aux logiciels qu'ils distribuent, et toutes les Parties Utilisatrices qui se fondent raisonnablement sur un Certificat Valide.
Garant d'un Certificat : personne désignée responsable pendant le cycle de vie du Certificat. Il peut s'agir ou non de la même entité que le Souscripteur.
Demande de Certificat : communications décrites à la Section 10.2 des Exigences de Base du CA/Browser Forum pour l'émission de Certificats Publiquement Reconnus (les « Exigences de Base ») afin de demander l'émission d'un Certificat.
Le Solliciteur : désigne le représentant du Demandeur qui a l'autorisation expresse de représenter le Demandeur, ou un tiers (tel qu'un FAI ou une société d'hébergement) qui remplit et soumet des Demandes de Certificat au nom du Demandeur. Les Souscripteurs de Certificat

peuvent être pré-approuvés grâce à la fonctionnalité d'un service de gestion GlobalSign, tel que la plate-forme MSSL ou EPKI.

Liste de Révocation des Certificats (« LRC ») : liste horodatée et régulièrement mise à jour des Certificats Électroniques Révoqués, créée et Signée Électroniquement par l'AC ayant émis les Certificats Électroniques.

Autorité de Certification (« AC ») : entité responsable de la création, l'émission, la révocation et la gestion des Certificats. Le terme désigne les AC Racines comme les AC Subordonnées. Désigne GlobalSign, ou toute entité certifiée par GlobalSign pour l'émission de Certificats au profit du « Sujet ». GlobalSign est l'AC du Demandeur aux termes des présentes.

Signature Electronique : encoder un message à l'aide d'un cryptosystème asymétrique et d'une fonction de hachage de façon à ce que la personne disposant du message initial et de la Clé Publique du signataire puisse définir avec exactitude si la transformation a été créée en utilisant la Clé Privée correspondant à la Clé Publique du signataire et si le message initial a été modifié depuis que la transformation a été effectuée. L'expression Signé Électroniquement s'applique aux données électroniques auxquelles une Signature Électronique a été annexée.

Nom de Domaine : étiquette attribuée à un nœud du Système de Noms de domaine.

Détenteur du Nom de Domaine : parfois désigné comme « propriétaire » du Nom de Domaine, mais plus exactement la(les) personne(s) ou l'(les) entité(s) enregistrée(s) auprès d'un Bureau d'Enregistrement de Noms de Domaine comme ayant le droit de contrôle sur la façon dont est utilisé un Nom de Domaine, telle que la Personne Morale ou physique enregistrée en tant que « Détenteur » par le Bureau d'Enregistrement des Noms de Domaine ou le service WHOIS.

Bureau d'Enregistrement des Noms de Domaine : personne ou entité qui enregistre les Noms de Domaine en vertu d'un contrat ou sous l'égide (i) de l'ICANN (Internet Corporation for Assigned Names and Numbers), (ii) d'une autorité ou d'un registre national de Noms de Domaines ou (iii) d'un NIC (Network Information Center ou centre d'information sur le réseau), y compris ses affiliés, sous-traitants, délégués, successeurs ou cessionnaires.

Système de Noms de Domaine : service Internet qui convertit les Noms de Domaine en adresses IP.

Nom de Domaine Complètement Qualifié : nom de Domaine qui comporte les étiquettes de tous les nœuds supérieurs du Système des Noms de Domaine Internet.

GlobalSign : entité de GlobalSign à laquelle le Souscripteur a passé un ordre d'achat d'un Certificat, qu'il s'agisse de GMO GlobalSign Limited, GMO GlobalSign, Inc., GMO GlobalSign Pte. Ltd, GMO GlobalSign Certificate Services Pvt. Ltd ou GMO GlobalSign Russia LLC.

Institution Publique : personne morale, agence, service, ministère, établissement ou autre organisme de même nature dans l'administration d'un pays ou une subdivision administrative d'un pays (telle qu'un État, une province, une ville, un département, etc.).

Compromission de clé : Une Clé privée est dite compromise si sa valeur a été divulguée à une personne non autorisée, si une personne non autorisée y a eu accès ou s'il existe une technique pratique permettant à une personne non autorisée d'en découvrir la valeur. On considère aussi qu'une Clé privée est compromise si certaines méthodes permettent d'en calculer la valeur sur la base de la clé publique (comme une clé Debian faible, voir http://wiki.debian.org/SSLkeys) ou si la méthode spécifique utilisée pour générer la Clé privée présente indéniablement des défauts.

Paire de Clés : la Clé Privée et sa Clé Publique associée.

Personne Morale : association, société, partenariat, entreprise individuelle, fiducie, entité publique ou autre entité disposant d'une personnalité juridique dans le système juridique d'un pays.

Exigences d'accréditations pour les Autorités de Certification homologuées du NAESB (North American Energy Standards Board) : critères techniques et organisationnels qu'une Autorité de Certification doit respecter pour être reconnue comme Autorité de Certification homologuée par le NAESB.

Online Certificate Status Protocol (« OCSP ») : protocole de vérification en ligne d'un Certificat qui permet à la Partie Utilisatrice d'une application logicielle de déterminer l'état d'un Certificat donné.

Clé Privée : dans une Paire de Clés, la clé qui est gardée secrète par le propriétaire de la Paire de Clés et sert à créer des Signatures Électroniques et/ou à décrypter des fichiers ou dossiers numériques ayant été cryptés avec la Clé Publique correspondante.
Clé Publique : dans une Paire de Clés, la clé qui peut être divulguée publiquement par le détenteur de la Clé Privée correspondante et est utilisée par une Partie Utilisatrice pour vérifier les Signatures Électroniques créées avec la Clé Privée correspondante du détenteur et/ou crypter des messages qui ne peuvent être décryptés qu'avec la Clé Privée correspondante du détenteur.
Autorité d'Enregistrement (« AE ») : personne Morale responsable de l'identification et de l'authentification des Sujets auxquels des Certificats sont attribués. Mais il ne s'agit pas d'une AC et, de ce fait, elle ne délivre, ni ne signe de Certificat. Une AE peut participer au processus de demande ou de révocation de Certificats ou aux deux. Lorsque « AE » est utilisé comme pour qualifier un rôle ou une fonction, l'entité désignée n'est pas forcément distincte, elle peut faire partie de l'AC.
Partie Utilisatrice : toute Personne Morale ou physique qui se fonde sur un Certificat Valide. Un Fournisseur d'Applications Logicielles n'est pas considéré comme une Partie Utilisatrice lorsqu'un logiciel distribué par ce fournisseur affiche simplement une information liée à un Certificat.
Certificat Racine : certificat auto-signé émis par l'AC Racine pour s'identifier et faciliter la vérification des Certificats délivrés à ses AC Subordonnées.
Sujet : personne Morale ou physique, appareil, unité ou système identifié dans un Certificat comme le Sujet. Le Sujet est soit le Souscripteur, soit un appareil exploité par un Souscripteur et sous son contrôle.
AC Subordonnée : autorité de Certification dont le Certificat est signé par l'AC Racine ou une autre AC Subordonnée.
Souscripteur : personne Morale ou physique à qui un Certificat est délivré et qui est juridiquement liée par un Contrat de Souscription ou des Conditions d'Utilisation.
Code Suspect : code contenant une fonction malveillante ou de sérieuses vulnérabilités, y compris les logiciels espions, malveillants ou tout autre code qui s'installe sans le consentement de l'utilisateur et/ou résiste à sa propre suppression, ou détection, et tout code susceptible d'être exploité d'une façon n'ayant pas été prévue par ses concepteurs, afin de compromettre la fiabilité des plates-formes sur lesquelles il s'exécute.
Conditions d'Utilisation : dispositions concernant la conservation et l'utilisation acceptable d'un Certificat, émises conformément aux Exigences de Base lorsque le Demandeur/Souscripteur est un Affilié de l'AC.
Certificat SSL Wildcard : certificat comportant un astérisque (*) à l'extrême gauche de chacun des Noms de Domaine Complètement Qualifiés du Sujet qu'il contient.

Les règles suivantes et directives associées sont intégrées par référence à ce Contrat.

- Déclaration sur les Pratiques de Certification (« DPC »). La version actuelle de la DPC est disponible sur http://www.globalsign.com/repository ; et
- Exigences de Base.

2.0 Autorisation d'utilisation des Certificats

2.1 Autorisation accordée : à compter de la Date de prise d'effet et pour la durée fixée dans le cadre de la période de validité de tout Certificat délivré (de la date de début de validité jusqu'à la date de fin de validité), GlobalSign accorde par les présentes au Souscripteur l'autorisation d'utiliser le Certificat conjointement à des utilisations de Clé Privée et/ou de Clé Publique. Les obligations du Souscripteur visées dans l'Article 4.0 en matière de protection des Clés Privées sont applicables à compter de la Date de prise d'effet.

2.2 Limitations de l'autorisation : le Souscripteur devra utiliser le Certificat uniquement avec des logiciels cryptographiques dotés d'une licence appropriée.

3.0 Services fournis par GlobalSign

Après acceptation du présent Contrat et après paiement des frais applicables, en sus de la « Délivrance de l'Autorisation », GlobalSign ou un tiers fournisseur désigné par GlobalSign devra fournir les services suivants à compter de la délivrance du Certificat.

3.1 Fourniture des Listes de Révocation des Certificats (LRC), des Services de Protocole de vérification en ligne du statut des Certificats (OCSP) et des informations relatives à l'Autorité émettrice du Certificat : GlobalSign devra fournir des efforts raisonnables afin de compiler, agréger et mettre à disposition sous format électronique, pour tous les Certificats signés et délivrés par l'AC GlobalSign, les informations suivantes :

- Les LRC de tous les Certificats contenant un point de distribution de Certificats de LRC,
- Les répondeurs OCSP pour tout Certificat contenant une URL de répondeur OCSP, et
- Les informations relatives aux Certificats émanant des points d'accès aux informations des Autorités ; sous réserve, toutefois, que GlobalSign n'enfreigne aucune de ses obligations aux termes des présentes en raison d'un retard d'exécution ou d'une non-exécution de sa part résultant du non-fonctionnement d'un équipement ou d'une panne de télécommunication survenant d'une façon raisonnablement indépendante de la volonté de GlobalSign.

3.2 Services de révocation pour les Certificats : la Révocation du Certificat d'un Souscripteur sera effectuée par GlobalSign dans les vingt-quatre (24) heures suivant l'un des évènements ci-dessous :

- Le Souscripteur demande par écrit la révocation du Certificat Électronique à l'entité de GlobalSign le lui ayant délivré ;
- Le Souscripteur informe GlobalSign que la Demande initiale de Certificat Électronique n'était pas autorisée et qu'il n'accorde pas rétroactivement cette autorisation ;
- GlobalSign obtient des preuves raisonnables qu'il y a eu Compromission de la Clé Privée du Souscripteur, ou que celle-ci ne répond plus aux exigences relatives au type d'algorithmes et à la taille de clé stipulées dans les Exigences de Base, ou que le Certificat a fait autrement l'objet d'une utilisation illicite ;
- GlobalSign est avisée de ou prend connaissance de la violation par le Souscripteur de l'une de ses obligations essentielles en vertu de ce Contrat de Souscription, ou des conditions d'utilisation ;
- GlobalSign est informée de tout évènement indiquant que l'utilisation d'un Nom de Domaine Complètement Qualifié ou d'une adresse IP du Certificat n'est plus autorisée juridiquement (c'est-à-dire qu'un arbitre ou un tribunal a révoqué le droit d'utilisation du Nom de Domaine par son Détenteur, qu'un contrat de services ou de licence concerné entre le Demandeur et le Titulaire du Nom de Domaine a été résilié ou que le Détenteur du Nom de Domaine n'a pas renouvelé le Nom de Domaine) ;
- GlobalSign est informée qu'un Certificat SSL Wildcard a été utilisé pour authentifier un Nom de Domaine Complètement Qualifié subordonné qui est frauduleux ou trompeur ;
- GlobalSign est avisée de ou prend connaissance de modifications importantes des informations contenues dans le Certificat;
- GlobalSign est informée que le Certificat émis ne respecte pas les Exigences de Base, la Politique de Certificats de GlobalSign ou cette DPC ;
- Si GlobalSign décide qu'une information apparaissant dans le Certificat n'est pas exacte, ou est trompeuse ;
- GlobalSign cesse ses activités pour quelque raison que ce soit et n'a pas pris de dispositions pour qu'une autre AC fournisse un support de révocation pour le Certificat ;
- Le droit de GlobalSign d'émettre des Certificats conformément aux Exigences de Base expire ou est révoqué ou résilié, sauf si GlobalSign a conclu des accords pour poursuivre la maintenance du Répertoire CRL/OSCP

- GlobalSign est informée d'une éventuelle Compromission de Clé d'une AC Subordonnée, ayant servi à l'émission du Certificat ;
- La révocation est exigée par la Politique de Certificats de GlobalSign et/ou sa DPC ;
- Le contenu technique du format du Certificat présente un risque inacceptable pour les Fournisseurs d'Applications Logicielles ou les Parties Utilisatrices (c'est-à-dire que le CA/Browser Forum peut décider qu'une taille de clé ou un algorithme de signature/cryptage obsolète présente un risque inacceptable et que ces Certificats doivent être révoqués et remplacés par les AC dans un délai donné) ; ou
- GlobalSign est informée que le Certificat a été utilisé pour signer un logiciel malveillant ou « malware ».

La révocation du Certificat d'un Souscripteur peut également être effectuée par GlobalSign dans un délai commercialement raisonnable, suivant l'un des évènements ci-dessous :

- Le Souscripteur ou l'administrateur de l'organisation demande la révocation du Certificat via un compte GCC (GlobalSign Certificate Center) qui contrôle le cycle de vie du Certificat ;
- Le Souscripteur demande la révocation du Certificat via une demande authentifiée transmise à l'Equipe d'assistance de GlobalSign ou à l'Autorité d'Enregistrement de GlobalSign ;
- GlobalSign est avisé de ou prend connaissance de la mise sur liste noire du Souscripteur en tant que personne interdite ou partie refusée, ou bien du fait qu'un Souscripteur opère depuis une destination interdite en vertu des lois en vigueur dans la juridiction opérationnelle de GlobalSign ;
- GlobalSign juge, à son entière discrétion, que l'utilisation du Certificat peut compromettre la sécurité ou la réputation de GlobalSign ou l'AC GlobalSign ou le niveau de confiance à leur égard ;
- À la suite d'une demande d'annulation d'un Certificat ;
- Si un certificat a été réémis, GlobalSign peut révoquer le Certificat émis précédemment ;
- Avec certains contrats de licence, GlobalSign peut révoquer les Certificats à l'expiration ou à la résiliation du contrat de licence applicable ;
- GlobalSign considère que la poursuite de l'utilisation du Certificat est autrement préjudiciable à l'activité de GlobalSign ou des parties tierces. Au moment de décider si l'utilisation d'un Certificat porte préjudice à l'activité ou la réputation de GlobalSign ou d'une partie tierce, GlobalSign examinera, entre autres, la nature et le nombre de plaintes reçues ; l'identité du/des plaignant(s) ; la législation en vigueur concernée, et les explications fournies par le Souscripteur concernant les accusations d'utilisation préjudiciable.
- Si Microsoft, à sa seule discrétion, identifie qu'un Certificat de Signature de Code ou de Signature de Code EV contient un nom fallacieux ou est utilisé pour promouvoir des logiciels malveillants ou indésirables, Microsoft contactera GlobalSign et lui demandera de révoquer le Certificat. GlobalSign révoquera le certificat dans un délai raisonnable sur le plan commercial ou demandera une exception auprès de Microsoft, dans les deux (2) jours suivant la réception de la demande de Microsoft. Microsoft peut accorder ou refuser l'exception à sa seule discrétion. Si Microsoft n'accorde pas l'exception, GlobalSign révoquera le certificat dans un délai raisonnable sur le plan commercial, qui ne dépassera pas deux (2) jours ouvrés ; ou
- Si Microsoft, à sa seule discrétion, identifie qu'un Certificat SSL est utilisé pour promouvoir des logiciels malveillants ou indésirables, Microsoft contactera GlobalSign et lui demandera de révoquer le Certificat. GlobalSign révoquera le certificat dans un délai raisonnable sur le plan commercial ou demandera une exception auprès de Microsoft dans les deux (2) jours suivant la réception de la demande de Microsoft. Microsoft peut accorder ou refuser l'exception à sa seule discrétion. Si Microsoft n'accorde pas l'exception, GlobalSign révoquera le certificat dans un délai raisonnable sur le plan commercial, qui ne dépassera pas deux (2) jours ouvrés.

3.3 Création des clés : si des Paires de clés sont créées par GlobalSign au nom du Souscripteur en étant offertes en tant que token ou options PKCS#12 ou AutoCSR, GlobalSign devra s'efforcer d'utiliser des systèmes fiables afin de créer ces Paires de Clés, auquel cas les conditions suivantes s'appliqueront. GlobalSign ne génère pas de Paires de Clés pour les certificats SSL de confiance publique :

- GlobalSign créera des Paires de Clés en recourant à des plates-formes reconnues pour être adaptées à un tel objectif et s'assurera que les Clés Privées sont chiffrées si elles sont transmises au Souscripteur,
- GlobalSign utilisera une longueur de clé et un algorithme reconnus pour être adaptés aux besoins de la Signature Numérique, et
- En présence de Certificats de Signature de Code et de Signature de Code EV, le Souscripteur accepte que GlobalSign ne signera pas de Paires de Clés inférieures à 2048 bits, et, en présence de Signature de Code EV, proposera SHA-2 comme seule option d'algorithme de signature.

3.4 Services de sceau de site pour les certificats SSL/TLS et les répondeurs OCSP/CRL : GlobalSign autorise le Demandeur à utiliser le sceau de site de GlobalSign sur le site web du Demandeur avec un taux quotidien maximum de cinq cent mille [500.000] impressions par jour. GlobalSign se réserve le droit de restreindre ou de mettre fin à la disponibilité du sceau si ladite limite est dépassée.

GlobalSign propose un service accessible 24 heures sur 24, 7 jours sur 7 permettant de vérifier la validité d'un certificat délivré à l'aide d'un répondeur OCSP ou de la liste de révocation de certificats (CRL). Le nombre maximum de validations est fixé à cinq cent mille [500.000] par certificat par jour. GlobalSign se réserve le droit de faire appliquer l'estampillage OCSP si cette limite est dépassée.

3.5 Services d'horodatage pour le Certificat de signature de code : GlobalSign offre la possibilité d'horodater du code signé à l'aide d'un Certificat de signature de code, ce service étant non facturable seulement si le service est utilisé raisonnablement. À titre de bonne pratique, GlobalSign exige que le Souscripteur horodate la signature électronique après avoir signé son code. GlobalSign fixe un nombre limite raisonnable d'opérations d'horodatage pendant la durée de validité du Certificat de Signature de Code et se réserve le droit de suspendre ce service ou de le facturer si elle estime que le volume d'opérations d'horodatage réalisé semble excessif.

3.6 Services d'horodatage pour le Certificat PDF Signing pour Adobe CDS : GlobalSign offre la possibilité d'horodater les documents PDF en tant que service payant de GlobalSign. Le nombre de signatures annuelles autorisées par ce service est établi pendant le processus de demande. GlobalSign se réserve le droit de retirer ce service ou de facturer des frais supplémentaires au titre de ce service si le volume d'opérations d'horodatage excède la limite convenue.

3.7 Services d'horodatage pour le Certificat AATL (Adobe Authorized Trust List) : GlobalSign peut offrir la possibilité d'horodater les documents Microsoft Office et PDF (Portable Document Format), à titre de service GlobalSign payant. Le nombre de signatures autorisées par an pour ce service est défini durant le processus de demande. GlobalSign se réserve le droit de suspendre le service ou facturer des frais supplémentaires pour celui-ci si le volume d'horodatages excède la limite convenue.

4.0 Obligations et Garanties du Souscripteur

Le Souscripteur et/ou Demandeur garantit au bénéfice de GlobalSign et des bénéficiaires des Certificats, ce qui suit :

4.1 Exactitude des informations : le Souscripteur s'engage à fournir à GlobalSign, à tout moment, des informations exactes, complètes et fiables, que ce soit dans la Demande de Certificat ou à la demande de GlobalSign en liaison avec l'émission d'un Certificat, y compris, sans caractère limitatif, le nom de l'application, l'URL d'information et la description de l'application liée aux Certificats de Signature de Code EV.

4.2 Protection des Clés Privées : le Demandeur s'engage à prendre toutes les mesures raisonnables pour garder un contrôle exclusif sur la Clé Privée à insérer dans le Certificat demandé , ainsi que tout service ou donnée d'activation lié (par ex. mot de passe ou jeton), en préserver la confidentialité et les protéger de façon appropriée à tout moment. Pour les Certificats de Signature de Code, le Souscripteur est tenu de fournir un réseau adéquat et d'autres contrôles de sécurité afin d'éviter l'utilisation abusive de la Clé Privée et la révocation du certificat sans avis préalable par GlobalSign en cas d'accès non autorisé aux Clés Privées.

4.3 Réutilisation de Clés Privées : pour les Certificats de Signature de Code, le Demandeur/Souscripteur n'est pas tenu de demander un Certificat de Signature de Code si la Clé Publique du Certificat est ou sera utilisée avec un Certificat autre que de Signature de Code.

4.4 Prévention des utilisations abusives : pour les Certificats de Signature de Code, le Souscripteur est tenu de fournir un réseau adéquat et d'autres contrôles de sécurité afin d'éviter l'utilisation abusive de la Clé Privée et la révocation du certificat sans avis préalable par GlobalSign en cas d'accès non autorisé aux Clés Privées.

4.5 Acceptation du Certificat : le Souscripteur s'engage à ne pas utiliser les Certificats avant que le Demandeur ou un agent du Demandeur n'ait examiné et vérifié l'exactitude de leur contenu.

4.6 Restrictions d'utilisation : le Souscripteur s'engage à installer le Certificat uniquement sur les serveurs accessibles par le(s) subjectAltName contenu(s) dans celui-ci et à ne s'en servir qu'en conformité avec toutes les lois applicables, le Contrat de Souscription et les Conditions d'Utilisation.

Si un Certificat est utilisé pour signer un PDF, le Souscripteur gardera l'information permettant de savoir qui a autorisé la signature de ce document particulier.

En aucun cas, le Certificat ne peut être utilisé à des fins délictuelles telles que des attaques de hameçonnage, des fraudes ou des certifications ou signatures de logiciels malveillants. Le Souscripteur s'engage à ne pas utiliser un Certificat pour signer sciemment un logiciel qui contient un Code Suspect ou pour distribuer autrement du contenu ayant pour effet de tromper, d'importuner ou d'ennuyer les destinataires, comme un logiciel comprenant des fonctions indésirables ou des programmes qui ne sont pas divulgués de façon appropriée à l'utilisateur avant l'installation, ou un logiciel qui est reconnu comme indésirable ou suspect par les applications commerciales de filtrage anti-virus.

Dans le cas des Certificats de signature de code à validation étendue, le souscripteur consent également à ces obligations et garanties supplémentaires :

- La signature de code ne doit être effectuée qu'en conformité avec les exigences énoncées dans le forum CA/Browser : directives relatives à l'émission et à la gestion des certificats de signature de code EV ;
- Uniquement en conformité avec toutes les lois applicables ;
- Uniquement pour les activités autorisées de l'entreprise ; et
- Uniquement en conformité avec le présent contrat.

Si le souscripteur est informé, d'une façon quelconque, qu'il a signé un code contenant un logiciel malveillant ou une vulnérabilité sérieuse, le souscripteur sera tenu d'en informer immédiatement GlobalSign.

Le Souscripteur reconnaît que Microsoft peut décider, de manière indépendante, qu'un Certificat est malveillant ou qu'il y a eu une Compromission de clé, et que les services et applications Microsoft auront la possibilité de modifier les expériences client Microsoft pour refléter cette décision de Microsoft, sans préavis et sans égard à l'état du Certificat au niveau de la révocation.

4.7 Informations et révocation : le Souscripteur est tenu de cesser immédiatement d'utiliser un Certificat et la Clé Privée qui lui est associée et de demander rapidement à l'AC de révoquer le Certificat s'il estime que (a) les informations dans le Certificat sont ou deviennent erronées ou inexactes, (b) la Clé Privée associée à la Clé Publique contenue dans le Certificat a été utilisée abusivement ou corrompue, ou (c) dans le cas d'un Certificat de Signature de Code, il y a des preuves que le Certificat a été utilisé pour signer un Code Suspect.

4.8 Résiliation de l'utilisation du Certificat : le Souscripteur devra cesser immédiatement d'utiliser la Clé Privée liée à la Clé Publique du Certificat lors de son expiration ou de sa révocation.

4.9 Réactivité : le Souscripteur sera tenu de répondre dans les quarante-huit (48) heures aux instructions de GlobalSign concernant la Compromission de clé ou l'utilisation abusive d'un Certificat.

4.10 Reconnaissance et Acceptation : le Souscripteur reconnaît et accepte que GlobalSign ait le droit de révoquer immédiatement le Certificat en cas de violation du Contrat de Souscription ou des Conditions d'Utilisation, ou si GlobalSign découvre que le Certificat a été utilisé pour permettre des activités délictuelles, telles que des attaques de hameçonnage, des fraudes ou la diffusion de logiciels malveillants.

S'agissant des Certificats de Signature de Code EV utilisés en liaison avec les applications et services de Microsoft, le Souscripteur reconnaît en outre que, même si un Certificat de Signature de Code EV peut ne pas être révoqué par GlobalSign, Microsoft peut, décider de façon indépendante, que le Certificat est compromis ou malveillant et modifier l'expérience client Microsoft dans les applications et services Microsoft concernés pour refléter sa décision, sans préavis ni égard à l'état du Certificat au niveau de la révocation.

4.11 Partage d'informations : en ce qui concerne les Certificats de Signature de Code, le Souscripteur reconnaît et accepte que, si (a) le Certificat ou le Demandeur est identifié comme étant une source de Code Suspect, (b) l'autorité pour la demande de Certificat ne peut pas être vérifiée ou (c) le Certificat est révoqué pour des raisons autres que la demande du Souscripteur (p. ex., à la suite d'une Compromission de clé, la découverte de logiciels malveillants, etc.), l'AC soit autorisée à communiquer des informations sur le Demandeur, la demande signée, le Certificat et les circonstances particulières à d'autres AC ou groupes du secteur, y compris le CA/Browser Forum..

4.12 Conformité aux normes du secteur : le Souscripteur reconnaît et accepte que GlobalSign puisse modifier le Contrat de Souscription, si nécessaire, pour se conformer à toute modification des Exigences Minimales pour l'Émission et la Gestion des Certificats de Signature de Code reconnus publiquement, publiées sur https://aka.ms/csbr, ou toute modification des Exigences de Base.

4.13 Contrôle de domaine exclusif pour les Certificats numériques SSL/TLS : le Souscripteur reconnaît et affirme avoir le contrôle exclusif du ou des noms de domaine ou de

l'adresse IP indiqués dans le ou les sous-domaines (SANs) pour lesquels il demande le Certificat SSL/TLS. S'il devait cesser d'avoir le contrôle exclusif d'un ou plusieurs noms de domaine, le Souscripteur doit en informer rapidement GlobalSign, conformément aux obligations visées à la section « Informations et révocation » ci-dessus.

4.14 Contrôle exclusif des emails pour le Certificat Electronique PersonalSign : le Souscripteur déclare et reconnaît avoir le contrôle exclusif de l'adresse email pour laquelle il/elle demande un Certificat PersonalSign. S'il ou si elle cesse d'avoir le contrôle exclusif d'une adresse email, le Souscripteur reconnaît qu'il/elle devra en informer GlobalSign sans délai conformément aux obligations visées dans l'Article ci-dessus intitulé « Informations et révocation ».

4.15 Création de Clés et utilisation : si des Paires de Clés sont créées par le Souscripteur ou le Solliciteur de Certificat, des systèmes fiables doivent être utilisés afin de créer des Paires de Clés, auquel cas les conditions suivantes s'appliqueront :
Les clés doivent être générées à l'aide d'une plate-forme reconnue comme adaptée à une telle fin. Dans le cas d'une signature PDF pour Adobe CDS, de la sécurité des e-mails et signature numérique de documents pour AATL et signature de code EV, celle-ci doit être conforme au niveau 2 de la norme FIPS 140-2
Une longueur de clé et un algorithme reconnus pour être adaptés aux besoins de la Signature Numérique doivent être utilisés, et
Le Souscripteur devra s'assurer que la Clé publique soumise à l'AC de GlobalSign correspond exactement à la Clé privée utilisée.

Lorsque des Paires de Clés sont créées avec un matériel conforme aux exigences du DPC :

- Le Souscripteur doit suivre des procédures, y compris, sans limitation, la modification des données d'activation, qui garantissent que chaque Clé privée au sein d'un HSM (Module Matériel de Sécurité) ou d'une clé USB cryptographique peut être utilisée uniquement avec les connaissances et l'action explicite du « Garant du Certificat»,
- Le Souscripteur doit s'assurer que le Garant du Certificat a reçu une formation de sécurité adaptée aux besoins pour lesquels le Certificat est délivré, et
- Les Garants du Certificat s'engagent à prendre toutes les mesures raisonnables nécessaires à l'exercice du contrôle exclusif, au respect de la confidentialité et à la protection appropriée, en toutes circonstances, de la Clé privée correspondant à la Clé publique devant être incluse dans le Certificat sollicité, ainsi que de tout mécanisme d'authentification associé permettant d'accéder à la clé - par exemple : un mot de passe pour une clé USB cryptographique ou un Module Matériel de Sécurité.
- Pour les Certificats de Signature de Code, le Souscripteur est tenu d'utiliser l'une des méthodes suivantes pour générer et protéger ses Clés Privées de Certificat de Signature de Code. GlobalSign recommande au Souscripteur d'utiliser la méthode 1 ou 2 de préférence à la méthode 3 :
  1. Une puce TPM (Trusted Platform Module) qui génère et sécurise une paire de clés et peut renseigner la protection des clés privées du Souscripteur par une attestation de clés TPM.
  2. Un module de chiffrement matériel avec un facteur de forme certifié conforme au moins à la norme FIPS 140 niveau 2, aux Critères Communs EAL 4+ ou l'équivalent.
  3. Un autre type de dispositif de stockage matériel avec un facteur de forme de carte SD ou de clé USB (pas nécessairement certifié conforme à la norme FIPS 140 niveau 2 ou aux Critères Communs EAL 4 +).

  Le Souscripteur garantit aussi qu'il conservera le dispositif de stockage séparé physiquement de l'appareil qui héberge la fonction de signature de code jusqu'au démarrage d'une session de signature.

- Pour les Certificats qualifiés, les Clés de l'abonné doivent être générées et stockées sur un dispositif certifié de création de signature qualifiée (QSCD) conforme aux exigences de l'annexe II du règlement (UE) n° 910/2014. L'Abonné accepte de n'utiliser le Certificat que dans le cadre d'un QSCD fourni ou approuvé par écrit par GlobalSign ; il appartient à l'Abonné de surveiller le statut de certification QSCD et les mesures appropriées devront être prises en cas de modification du statut de certification du QSCD.

4.16 Certificats NAESB :

Les souscripteurs de certificats NAESB (« North American Energy Standards Board ») attestent avoir compris les obligations suivantes envers les normes WEQ PKI par l'intermédiaire de GlobalSign.

Les entités finales engagées à respecter la norme de pratique commerciale WEQ-012 v3.0 devront s'inscrire au registre des industries électriques du NAESB et fournir la preuve de leur autorisation à prendre part au secteur de l'électricité de gros. Les entités ou organisations susceptibles de nécessiter l'accès à des applications faisant appel à l'authentification spécifiée dans le cadre de la norme de pratique commerciale WEQ-012 du NAESB, mais n'étant pas considérées comme acteur du marché de l'électricité de gros (par exemple, les organismes de réglementation, universités, cabinets de consultants, etc.), ont l'obligation de s'inscrire.

Les entités finales enregistrées et la communauté d'utilisateurs qu'elles représentent sont tenues de respecter toutes les obligations des entités finales énoncées dans les Normes WEQ PKI.

L'organisation du Souscripteur devra certifier à GlobalSign qu'elle a examiné et accepte les Normes WEQ PKI suivantes :

4.16.1 L'entité du Souscripteur reconnaît le besoin du secteur de l'électricité de sécuriser les communications électroniques privées facilitant les objectifs suivants :

- **La confidentialité :** la garantie pour une entité qu'aucun individu ne puisse lire un élément de données particulier à l'exception du ou des destinataires (s) explicitement concernés ;
- **L'authentification :** la garantie pour une entité qu'une autre entité est effectivement celui/celle qu'il/elle prétend être ;
- **L'intégrité :** la garantie pour une entité que les données n'ont pas été modifiées (intentionnellement ou non) entre « là-bas » et « ici », ou entre « hier » et « aujourd'hui » ; et
- **La non-répudiation :** Une partie ne peut nier avoir participé à l'opération ou avoir envoyé le message électronique.

4.16.2 Le Souscripteur reconnaît l'approbation de l'industrie de la cryptographie par Clé Publique qui fait appel à des Certificats, afin de lier la Clé Publique d'une personne ou d'un système informatique à son entité, et pour prendre en charge l'échange de clés par chiffrement symétrique.

4.16.3 Le Souscripteur a passé en revue les normes WEQ PKI contenant les règles du secteur relatives à l'établissement d'une infrastructure à clés publiques (PKI) de confiance.

4.16.4 Le Souscripteur a évalué la Déclaration des Pratiques de Certification de GlobalSign, compte tenu des normes du secteur telles que définies par GlobalSign.

S'il y a lieu, les Souscripteurs sont tenus d'enregistrer leur identification commercial légale, ainsi que de se procurer un « code d'entité » qui sera publié dans le registre des industries électriques du NAESB, et utilisé dans toutes les applications des souscripteurs soumises par, et tous certificats délivrés à, cette entité finale. Pour le respect des normes WEQ-012 lors de l'émission de Certificats à utiliser dans le secteur de l'énergie pour les demandes autres que WEQ-012, les agents de l'AC sont tenus de se conformer aux dispositions des normes WEQ PKI, sauf les dispositions stipulées dans WEQ-012.12.1.9, WEQ-012-1.3.3 et WEQ-012.1.4.3, qui exigent l'enregistrement de l'entité finale dans le registre des industries électriques du NAESB.

Les Souscripteurs sont également tenus de se conformer aux exigences suivantes :

- Protéger leurs Clés Privées de l'accès par d'autres parties.
- S'il y a lieu, identifier, grâce au registre des industries électriques du NAESB, qu'ils ont choisi GlobalSign comme Autorité de Certification Agréée
- Mettre en application l'ensemble des accords et contrats passés avec GlobalSign, tel que requis par la DPC de GlobalSign, pour que ce dernier soit en mesure de délivrer des certificats à l'entité finale en vue de la sécurisation des communications électroniques.
- Se conformer à toutes les obligations demandées et prévues par GlobalSign dans la DPC, c'est-à-dire, les procédures de demande de Certificat, la vérification d'identité du Demandeur, ainsi que les pratiques de gestion des Certificats.
- Confirmer l'existence d'un programme de gestion des Certificats, la formation de tous les employés concernés au sein de ce programme, et la mise en place de contrôles destinés à garantir la conformité avec ce programme. Ce programme doit inclure, mais sans s'y limiter :
  - la ou les politiques de sécurité et de gestion des Clés Privées de Certificats
  - la ou les politiques de révocation de Certificats
- Identifier le type de Souscripteur (c'est-à-dire, individu, rôle, périphérique ou application) et fournir des renseignements complets et exacts pour chaque Demande de certificat.

5.0 Consentement de publication des informations

Par le simple fait de fournir des informations à caractère personnel lors de la demande d'un Certificat, le Souscripteur consent à ce que GlobalSign communique publiquement ces informations (i) en les intégrant dans le Certificat émis et (ii) en publiant le Certificat dans les journaux de Transparence des Certificats (CT).

6.0 Limitation de garantie

SAUF DANS LA MESURE PROHIBÉE PAR LA LOI OU TOUTE DISPOSITION CONTRAIRE DANS LE PRÉSENT DOCUMENT, GLOBALSIGN RÉFUTE TOUTE GARANTIE, Y COMPRIS TOUTE GARANTIE DE VALEUR MARCHANDE ET/OU D'ADÉQUATION À UN OBJECTIF PARTICULIER.

DANS LA MESURE OÙ GLOBALSIGN A ÉMIS ET GÉRÉ LE CERTIFICAT CONFORMÉMENT AUX EXIGENCES DE BASE ET À LA DPC, GLOBALSIGN NE SERA PAS RESPONSABLE ENVERS LE SOUSCRIPTEUR, LES PARTIES UTILISATRICES OU TOUT TIERS, POUR TOUTE PERTE SUBIE DU FAIT DE L'UTILISATION DE CE CERTIFICAT OU DE LA CONFIANCE LUI AYANT ÉTÉ ACCORDÉE. AUTREMENT, LA RESPONSABILITÉ DE GLOBALSIGN ENVERS LE SOUSCRIPTEUR, LA PARTIE UTILISATRICE OU TOUT TIERS POUR CES PERTES NE DÉPASSERA EN AUCUN CAS MILLE DOLLARS (1 000 $) PAR CERTIFICAT, SOUS RÉSERVE CEPENDANT QUE CETTE LIMITATION SOIT DE DEUX MILLE DOLLARS (2 000 $) PAR CERTIFICAT POUR UN CERTIFICAT EV OU UN CERTIFICAT DE SIGNATURE DE CODE EV.

CE PLAFOND DE RESPONSABILITÉ LIMITE LES DOMMAGES RECOUVRABLES EN DEHORS DU CONTEXTE DE LA POLITIQUE DE GARANTIE DE GLOBALSIGN. LES SOMMES PAYÉES DANS LE

CADRE DE LA POLITIQUE DE GARANTIE SONT SOUMISES À LEURS PROPRES PLAFONDS DE RESPONSABILITÉ.

EN AUCUN CAS, GLOBALSIGN NE POURRA ÊTRE TENUE RESPONSABLE DE TOUT DOMMAGE INDIRECT, ACCESSOIRE, PARTICULIER OU CONSÉCUTIF OU DE TOUTE PERTE DE PROFITS, PERTE DE DONNÉES OU AUTRE DOMMAGE INDIRECT, ACCESSOIRE OU CONSÉCUTIF RÉSULTANT DE/LIÉ À L'UTILISATION, LA REMISE, LE RECOURS, LA LICENCE OU DU/AU FONCTIONNEMENT OU NON-FONCTIONNEMENT DES CERTIFICATS, SIGNATURES ÉLECTRONIQUES OU AUTRES TRANSACTIONS OU SERVICES OFFERTS OU ENVISAGÉS PAR CETTE DPC, NI DE LA CONFIANCE QUI Y A ÉTÉ PLACÉE.

LA LIMITATION DE RESPONSABILITÉ SERA IDENTIQUE, QUEL QUE SOIT LE NOMBRE DE SIGNATURES ÉLECTRONIQUES, TRANSACTIONS OU PLAINTES LIÉES AU CERTIFICAT ÉLECTRONIQUE CONCERNÉ.

7.0 Durée et résiliation

Le présent Contrat prendra fin à la survenue du premier des cas suivants :

- A la date d'expiration du Certificat délivré au Souscripteur, directement, indirectement ou par le biais d'un service MSSL ou EPKI qui n'a pas encore expiré ; ou
- En cas de non-exécution par le Souscripteur de l'une de ses obligations essentielles en vertu du présent Contrat s'il n'est pas porté remède à un tel manquement dans un délai de cinq (5) jours à compter de la réception de la notification correspondante envoyée par GlobalSign.

8.0 Conséquences de la Résiliation

Lors de la résiliation du présent Contrat pour quelque motif que ce soit, le Certificat du Souscripteur pourra être révoqué par GlobalSign conformément aux procédures de GlobalSign. Lors de la révocation du Certificat du Souscripteur, toute autorisation accordée au Souscripteur en vertu de l'Article 2 des présentes prendra fin. Ladite résiliation n'affectera pas les Articles 4, 5, 6, 8 et 9 du présent Contrat qui conserveront toute leur force exécutoire dans la mesure de ce qui est nécessaire à leur bonne et entière exécution.

9.0 Dispositions diverses

9.1 Droit applicable

Si vous avez passé votre commande auprès de GMO GlobalSign Limited, le présent Contrat sera régi par et interprété selon les lois d'Angleterre et du Pays de Galles nonobstant ses dispositions relatives au conflit des lois. La juridiction compétente sera celle de l'Angleterre.

Si vous avez passé votre commande auprès de GMO GlobalSign Inc., le présent Contrat sera régi par et interprété selon les lois de l'Etat du New Hampshire aux USA nonobstant ses dispositions relatives au conflit des lois. La juridiction compétente sera celle de l'Etat du New Hampshire.

Si vous avez passé votre commande auprès de GMO GlobalSign Pte. Ltd., le présent Contrat sera régi par et interprété selon les lois de Singapour nonobstant ses dispositions relatives au conflit des lois. La juridiction compétente sera celle de Singapour.

Si vous avez passé votre commande auprès de GMO GlobalSign Certificate Services Pvt. Ltd, le présent Contrat sera régi par, et interprété en vertu du et conformément au droit indien et aux lois étatiques connexes, indépendamment des dispositions légales en matière de conflit d'intérêt. La juridiction compétente sera celle de l'Inde.

Si vous avez passé votre commande auprès de GMO GlobalSign Russia LLC, le présent Contrat sera régi par, et interprété en vertu du et conformément au droit de la Fédération de Russie, indépendamment des dispositions légales en matière de conflit d'intérêt. La juridiction compétente sera celle de la Fédération de Russie.

9.2 Force obligatoire

Sauf disposition contraire dans les présentes, le présent Contrat aura force obligatoire pour les successeurs, liquidateurs, héritiers, représentants, administrateurs et ayant droits des parties aux présentes et s'appliquera à leur profit. Ni le présent Contrat ni les droits du Souscripteur envers le Certificat ne pourront être cédés par le Souscripteur. Toute cession ou délégation alléguée sera de nul effet et donnera motif à GlobalSign de mettre fin au présent Contrat.

9.3 Intégralité de l'accord

Le présent Contrat, ainsi que tous les documents qui sont référencés dans ce dernier, tout Contrat de service ou de produit, et le Contrat pour Revendeurs (si vous êtes un Revendeur) forment l'intégralité du Contrat entre les parties et a préséance sur tout accord précédent, verbal ou écrit, toute promesse, interprétation, verbales ou écrites, conclu entre les parties ou les communications relatives au contenu même du Contrat.

9.4 Divisibilité

Dans le cas où l'une des dispositions du présent Contrat, ou son application, s'avérerait pour un motif et dans une mesure quelconque, non valable ou non-exécutoire, le reste du présent Contrat et l'application des dispositions concernées à l'égard d'autres personnes ou circonstances seront interprétés de façon à permettre au mieux et de manière raisonnable la réalisation de l'objet fixé par les parties aux présentes. IL EST EXPRESSEMENT CONVENU ET ACCEPTE QUE CHAQUE DISPOSITION DU PRESENT CONTRAT STIPULANT UNE LIMITATION DE RESPONSABILITES, DE GARANTIES, OU UNE EXCLUSION DE DOMMAGES, EST DESTINEE PAR LES PARTIES AU PRESENTES A ETRE DISSOCIABLE ET INDEPENDANTE DE TOUTE AUTRE DISPOSITION ET A ETRE APPLIQUEE EN TANT QUE TEL.

9.5 Notifications

Lorsque le Souscripteur décide ou se voit demander d'adresser une notification ou une demande à GlobalSign relativement au présent Contrat, chacune de ces communications devra être établie par écrit et ne sera effective que si elle est remise par un service de messagerie confirmant ladite remise par écrit ou par courrier transmis par voie postale, par courrier certifié ou recommandé, avec affranchissement prépayé, avec demande d'accusé de réception, adressé à GlobalSign à l'un de nos bureaux internationaux listés sur :
http://www.globalsign.com/company/contact.htm, à l'attention du Service Juridique.
Lesdites communications seront dites effectives à compter de leur réception.

9.6 Confidentialité - Utilisation de bases de données de tiers

GlobalSign est tenu de suivre la politique de confidentialité publiée sur son site web lors de la réception et de l'utilisation des informations du Souscripteur. GlobalSign peut modifier sa politique de confidentialité à tout moment en publiant la version modifiée sur son site web.

Par le simple fait de fournir des informations à caractère personnel lors de la demande d'un Certificat, le Souscripteur consent à ce que GlobalSign traite ces informations, les communique et les transfère à l'échelle mondiale à ses sociétés affiliées, agents et sous-traitants si nécessaire pour valider et émettre un Certificat, et consent également au traitement, à la communication et au transfert dans des pays dont les lois sur la protection des données peuvent être moins protectrices que celles du pays où est situé le Souscripteur.

Pour les personnes physiques, GlobalSign peut valider des données telles que le nom, l'adresse et autres informations personnelles fournies au cours de la procédure de demande à l'aide de bases de données tierces appropriées. En concluant le présent Contrat, le Souscripteur accepte que de telles vérifications soient effectuées. Lors de la réalisation desdites vérifications, des informations personnelles fournies par le Souscripteur peuvent être divulguées auprès d'agences agréées d'évaluation du crédit, lesquelles pourront conserver lesdites informations. Ces vérifications ne sont effectuées qu'aux fins de confirmation de l'identité et à cet égard il est précisé qu'aucun contrôle de solvabilité n'est effectué. L'évaluation de la solvabilité du Souscripteur n'est en aucun cas affectée par cette procédure.

Si vous avez passé votre commande auprès de GMO GlobalSign Russie LLC, GlobalSign a la possibilité, pour les personnes physiques, de valider des éléments, tels que le nom, l'adresse et toute autre information personnelle fournie lors de la demande. En concluant le présent Contrat, l'abonné consent au traitement de ses données personnelles par GlobalSign comme suit : la collecte, le classement, le traitement, le stockage, la modification, l'utilisation, la dépersonnalisation, le blocage et la suppression, comme stipulé par la loi fédérale russe FZ-No.152 au 27/07/2006, ainsi que le transfert à des tiers dans les cas prévus par la réglementation des instances supérieures et par la loi.

9.7 Marques commerciales et logos

Au titre du présent Contrat ou de l'exécution de celui-ci, le Souscripteur et GlobalSign n'acquerront aucun droit d'aucune sorte sur aucune marque commerciale, nom commercial, logo ou désignations de produits de l'autre partie ni ne feront aucune utilisation de ces derniers pour quelque motif que ce soit sauf autorisation écrite de la partie propriétaire de tous les droits relatifs auxdites marques commerciales, noms commerciaux, logos ou désignations de produits concernés.

10.0 Assistance

Le Souscripteur est tenu d'avertir immédiatement GlobalSign par l'intermédiaire de l'un de ses bureaux, dont la liste figure sur https://www.globalsign.fr/fr/entreprise/contact/, en cas d'erreur dans un Certificat. Si le Souscripteur n'agit pas dans les sept (7) jours suivant la réception du Certificat, celui-ci sera réputé avoir été accepté.

GlobalSign procèdera à des remboursements selon la Politique de Remboursement de GlobalSign publiée sur https://www.globalsign.fr/fr/informations-juridiques/

Filename: Contrat de souscription GlobalSign - Version 3.8.doc
Directory: \\kenfs01.internal.globalsign.com\Marketing\Public\Marketing\Legal docs\French
Template: C:\Users\stephanie.gallet\AppData\Roaming\Microsoft\Templates\Normal.dotm
Title:
Subject:
Author: Steve Roylance
Keywords:
Comments:
Creation Date: 06/04/2018 11:43:00
Change Number: 7
Last Saved On: 25/06/2018 14:53:00
Last Saved By: Stephanie Gallet
Total Editing Time: 66 Minutes
Last Printed On: 25/06/2018 14:53:00
As of Last Complete Printing
Number of Pages: 14
Number of Words: 7,581 (approx.)
Number of Characters: 43,212 (approx.)