CONDITIONS PARTICULIERES – CERTIFICAT SSL

Version en date du 22/10/2019

PREAMBULE

Les présentes Conditions Particulières sont conclues entre :

- la société OVH, SAS, société de droit Français, élisant domicile 2 rue Kellermann 59100 Roubaix, inscrite au RCS de LILLE METROPOLE sous le numéro B 424 761 419, représentée par M. Henryk KLABA Président, ci- après dénommée : « OVH »

- et toute personne morale ou physique, particulier ou professionnel, de droit privé ou de droit public, souhaitant procéder à la souscription d'un Certificat SSL, ci-après dénommée : "le Client".

ARTICLE 1 – OBJET

Les présentes Conditions Particulières et leurs Annexes, complétant les Conditions Générales de Service d'OVH, ont pour objet de définir les conditions techniques et financières dans lesquelles OVH s'engage à fournir au Client un Certificat Electronique associé au Nom de Domaine de son choix.

Les présentes Conditions Particulières et ses Annexes prévaudront sur les Conditions Générales si une contradiction devait apparaître entre ces documents.

ARTICLE 2 – DEFINITIONS ET INTERPRETATIONS

Dans les présentes Conditions Particulières et sauf lorsque le contexte l'exige autrement, les termes et expressions sous-mentionnés ont la signification suivante :

« **Certificat SSL** » (également appelé un « Certificat ou Certificat Electronique ») : SSL est l'acronyme anglais de « Secure Socket Layer ». Il désigne un protocole standard de sécurisation de la transmission de données sur Internet. Un Certificat SSL est un Certificat numérique qui est une suite de données liant cryptographiquement un titulaire identifié par sa Clé Privée à une Clé Publique. Un Certificat SSL peut être attribué à un individu, une organisation privée ou gouvernementale, un établissement d'enseignement, ou à un composant de réseau informatique, tel que le pare-feu, un routeur, ou tout autre support matériel de sécurité.

« **Signature Numérique** » signifie un fichier de données électronique chiffré qui est joint ou lié logiquement à une autre donnée électronique, qui identifie et est uniquement rattaché à la signature de la donnée électronique, qui est créé grâce à la Clé Privée du signataire et est lié de manière à pouvoir effectuer des modifications ultérieures sur les données électroniques détectables.

« **Clé Privée** » signifie un fichier de données électronique chiffré et confidentiel conçu pour être en liaison avec une Clé Publique utilisant le même algorithme de chiffrage et qui peut être utilisé pour créer des signatures numériques, pour déchiffrer des fichiers ou des messages qui ont été chiffré avec une Clé Publique.

« **Clé Publique** » signifie un fichier de données électronique chiffré et librement disponible qui est conçu pour être en liaison avec une Clé Privée utilisant le même algorithme de chiffrage et qui peut être utilisé pour vérifier les Signatures Numériques et pour chiffrer des fichiers ou des messages.

« **Nom de Domaine** » chaine de caractères (ex :ovh) associée à une extension (ex : .com, .fr...) constituant un nom familier associé à une adresse IP.

« **Serveur** » signifie le Serveur du Client fonctionnant avec l'adresse IP identifiée par un Nom de Domaine par le Client à OVH et qui est lié de manière chiffrée à la Clé Publique présentée dans le Certificat SSL.

ARTICLE 3 – ACCES AU SERVICE ET CONDITION DE REALISATION DES PRESTATIONS

OVH propose le service de Certificat SSL dans le cas où le Client dispose d'un Nom de Domaine.

Toute souscription par le Client à une prestation d'abonnement à un Certificat SSL OVH, implique la création par celui-ci d'un compte auprès d'OVH. Toute passation, modification ou annulation de commande réalisée à partir de ce compte se fait sous l'entière responsabilité du Client.

Les services d'hébergement compatibles avec le service de Certificat SSL sont renseignés sur le site Internet d'OVH (https://www.ovh.com/).

Le Client reconnaît que le Certificat SSL est lié au Nom de Domaine qu'il a choisi. En ce sens, il n'est pas transférable d'un Nom de Domaine à un autre, souscrit auprès d'OVH ou d'un bureau d'enregistrement tiers, au cours ou au terme du contrat.

ARTICLE 4 – OBLIGATIONS ET RESPONSABILITE DU CLIENT

Le Client mandate OVH pour agir en tant qu'intermédiaire auprès de l'Autorité de Certification notamment pour accepter les accords de souscription avec l'Autorité de Certification et procéder à la confirmation de sa commande auprès de l'Autorité de Certification. Le Client

autorise expressément OVH à transmettre à l'Autorité de Certification toute information qui lui serait demandée dans le cadre strict de la fourniture du service de Certificat SSL.

L'Autorité de Certification procédera au processus de validation du Certificat SSL demandé par le Client. Le Client sera directement contacté par l'Autorité de Certification.
OVH rappelle au Client que celui-ci doit, dans le cadre de la fourniture du service de Certificat SSL, communiquer à OVH ses coordonnées exactes et régulièrement mises à jour. Le Client reconnaît que le Certificat Electronique est susceptible de faire l'objet d'une annulation par OVH ou par l'Autorité de Certification dans le cas où le Client fournirait des coordonnées et des informations incorrectes.

Le Client s'engage à être seul responsable de l'espace d'hébergement du site sur lequel est installé le Certificat Electronique et de disposer des accès permettant sa gestion.

Le Client s'oblige à obtenir toute autorisation, permission ou licence qui lui serait nécessaire pour utiliser le Certificat SSL et le maintenir en vigueur.

Le Client devra prendre toutes les précautions adéquates pour empêcher toute violation, perte de contrôle ou divulgation non autorisée d'informations confidentielles dès la remise de sa Clé Privée.

Le Client ne devra pas utiliser le Certificat SSL souscrit pour transmettre (aussi bien par l'envoi de courriels que par un téléchargement qui utilise toute forme de protocole de communication), recevoir (aussi bien en sollicitant un courriel que par un téléchargement qui utilise toute forme de protocole de communication), divulguer, afficher ou utiliser de toute autre façon des informations qui seraient illégales, offensantes, abusives, contraires à la moralité publique, indécentes, diffamatoires, obscènes ou menaçantes, ou qui violeraient toute confiance, tout droit d'auteur ou autre droit de propriété intellectuelle d'un tiers, qui peineraient, embarrasseraient, causeraient un déni de service, une perturbation ou des troubles. Il ne devra pas envoyer ou proposer des matériaux publicitaires ou promotionnels ou toute autre forme de correspondance non sollicitée.

Le Client s'engage à utiliser le Certificat SSL raisonnablement, au sens des dispositions du code civil mais également de la jurisprudence actuelle.

ARTICLE 5 – OBLIGATIONS ET RESPONSABILITE D'OVH

OVH s'engage à apporter tout le soin et la diligence nécessaires à la fourniture d'un service de qualité conformément aux usages de la profession et à l'état de l'art. Il ne répond que d'une obligation de moyens.

Les obligations d'OVH au titre des présentes Conditions Particulières se bornent à un rôle d'intermédiaire entre le Client et le prestataire fournissant le Certificat SSL, à savoir l'Autorité de Certification.

OVH peut, à sa seule discrétion et après avoir prévenu le Client au minimum trente (30) jours à l'avance par ses moyens de communication habituels (listes de diffusion, forums, site Internet www.ovh.com), procéder à la modification ou à la résiliation du service de Certificat SSL dans le cas où l'Autorité de Certification cesse ses opérations ou ne dispose plus du droit de délivrer des Certificats SSL.

ARTICLE 6 – MODALITES DE PAIEMENT

Le montant que le Client devra verser à OVH au titre du service de Certificat SSL souscrit sera exposé sur le site Internet d'OVH durant la procédure de commande. Ce montant devra être versé par le Client immédiatement lors de la commande.

OVH tient à rappeler que son rôle est celui d'intermédiaire auprès de l'Autorité de Certification. Ainsi, si lors du processus de vérification aux conditions d'éligibilité d'un Certificat SSL, l'Autorité de Certification refuse de délivrer le Certificat Electronique, OVH n'est aucunement responsable. Aucun paiement versé par le Client à OVH au titre du service de Certificat SSL souscrit ne sera remboursable.

ARTICLE 7 – DUREE DU CONTRAT ET EXPIRATION DU SERVICE

Le Service est souscrit par le Client pour une durée d'un (1) an à trois (3) ans à compter de la date d'émission du Certificat SSL pour les Certificats DV et OV. Et une durée d'un (1) an à deux (2) ans pour les Certificats EV à compter de la date d'émission du Certificat SSL. Le Client sera notifié par OVH de l'expiration de son Certificat SSL. Le Client recevra une notification soixante (60) jours, trente (30) jours, quinze (15) jours, sept (7) jours et trois (3) jours avant l'expiration de son Certificat SSL. OVH ne sera pas tenu responsable si le Client n'a pas renouvelé son Certificat SSL dans le temps imparti. Le Client recevra également une notification le jour de l'expiration de son Certificat SSL.

Afin de renouveler son Certificat SSL, le Client devra procéder à une nouvelle commande, qui sera soumise au même processus de validation que la commande initiale.

En revanche, un Certificat SSL révoqué ne peut pas être renouvelé.

Un Certificat SSL peut être résilié sur le champ ou à la date spécifiée dans le préavis : par chaque partie si l'autre commet une infraction importante d'une condition des présentes Conditions Particulières et que cette dernière (dans le cas d'une infraction pouvant être remédiée) n'est pas remédiée dans les vingt (20) jours ouvrés suivant une demande écrite de

l'autre partie demandant la résolution du litige, ou par chaque partie s'il se produit un problème d'insolvabilité chez l'autre partie ou que cette autre partie cesse d'exercer ses activités.

Seul le titulaire du Certificat SSL est autorisé à solliciter la révocation de ce dernier à tout moment, y compris avant son expiration. Dans un tel cas, le Client doit immédiatement cesser d'utiliser son Certificat SSL. OVH ne procédera à aucun remboursement. OVH ne sera pas tenu responsable pour les pertes et préjudices causés lors de période de temps entre la demande de révocation faite par le Client et l'effective révocation exécutée par OVH.

ARTICLE 8 – LIMITATION DE LA RESPONSABILITE

LE CLIENT ACCEPTE EGALEMENT QU'EN AUCUN CAS OVH NE SERA TENU POUR RESPONSABLE ENVERS LE CLIENT POUR TOUTE PERTE ENCOURUE PAR CE DERNIER DU FAIT DE L'UTILISATION DU CERTIFICAT SSL EN DEHORS DU CHAMP D'UTILISATION TEL QU'IL EST SPÉCIFIÉ DANS LES PRESENTES CONDITIONS PARTICULIERES.

LE CLIENT RECONNAIT AUSSI QUE OVH NE SERA PAS TENU POUR RESPONSABLE VIS- A-VIS DU CLIENT POUR TOUTE PERTE, COMPRENANT TOUS DOMMAGES INDIRECTS, ACCIDENTELS, SPÉCIFIQUES OU SECONDAIRES, ENCOURUS PAR CHAQUE PARTIE EN RAISON D'UNE PERTE, D'UN VOL, D'UNE DIVULGATION NON AUTORISÉE, D'UNE MANIPULATION NON AUTORISÉE, D'UNE ALTÉRATION, D'UNE PRIVATION DE JOUISSANCE OU DE TOUT AUTRE COMPROMISSION CONCERNANT TOUTE CLÉ PRIVÉE UTILISÉE PAR LE CLIENT.

ARTICLE 9 - MODIFICATION DU CONTRAT

Conformément aux Conditions Générales de Service d'OVH, et selon les modalités qui y sont prévues, les présentes Conditions Particulières sont susceptibles d'être modifiées afin de prendre en compte notamment toute évolution jurisprudentielle, légale ou technique, ou règles établies par l'Autorité de Certification.

ARTICLE 10 – DROIT DE RETRACTATION

Conformément aux dispositions de l'article L 221-28 3° du Code de la Consommation « *le droit de rétractation ne peut être exercé (...) pour les contrats de fourniture de biens confectionnés selon les spécifications du consommateur ou nettement personnalisés (...)* ».
Le Client reconnaît que la création du Certificat SSL pour son Nom de Domaine constitue, une fourniture d'un tel bien personnalisé au sens de l'article précité.

Dès lors, le Client est expressément informé qu'il ne peut, en application de ces dispositions, exercer son droit de rétractation sur ce Service. Ce droit ne peut davantage être exercé par le Client lors du renouvellement du Service.

ANNEXES N° 1 – PROCEDURE DE VALIDATION DES CERTIFICATS SSL

1- DOMAIN VALIDATED CERTIFICATES (DV)

Le Nom de Domaine associé au Certificat SSL doit être vérifié au travers de l'une des trois procédures suivantes :

- Vérification par email
- Vérification par http
- Vérification par Nom de Domaine

Des détails additionnels peuvent être trouvés à l'adresse suivante :
https://support.sectigo.com/Com_KnowledgeDetailPageFaq?Id=kA01N000000brbt

2- ORGANIZATION VALIDATED CERTIFICATES (OV)

Première étape : Si le Client est une organisation (société, association, agence gouvernementale, etc.), son identité doit impérativement être vérifiée. Et cela au travers de l'une des quatre procédures suivantes :

- Grace à une agence gouvernementale basée dans la juridiction où le client a procédé à sa création légale.
- Grace à une base de données tierce, mise à jour régulièrement.
- Une attestation légale.
- Une visite du site du Client par l'Autorité de Certification ou un tiers agissant comme agent de cette dernière.

Une fois cette vérification confirmée, l'adresse de l'organisation doit être vérifiée. Cinq procédures sont possibles :

- Consulter les articles de constitution.
- Copie d'une facture de téléphone récente de l'organisation.
- Copie de l'actuel bail de l'organisation ou encore d'une facture considérée comme nécessaire (eau, électricité, gaz, etc.).
- Un extrait de KBIS ou équivalent.
- Une copie d'un RIB récent de l'organisation.

Si le Client est une personne physique, son identité doit aussi être vérifié et cela en fournissant une copie de sa pièce d'identité (passeport, permis de conduire, carte nationale d'identité ou équivalent). Son adresse doit également être vérifiée en fournissant une copie d'une facture récente.

Par « récent », on entend un délai inférieur à six mois.

Deuxième étape : Vérification du Whois associé.
Troisième étape : Le Nom de Domaine associé au Certificat SSL doit être vérifié au travers de l'une des trois procédures suivantes :

- Vérification par adresse électronique
- Vérification par http
- Vérification par Nom de Domaine

Quatrième étape : Vérification téléphonique. Le numéro de téléphone fourni par le Client doit être vérifié au travers de l'un des moyens suivants :

- Le numéro apparaît sur une base de données gouvernementale ;
- Le numéro apparaît sur une autre base de données ;
- Le numéro apparaît sur une facture de téléphone.

Si toutes les étapes peuvent être validées, le Certificat SSL sera signé et délivré.

3- EXTENDED VALIDATED CERTIFICATES (EV)

Première étape : L'Autorité de Certification doit s'assurer que l'organisation est active. Cette procédure varie en fonction du pays d'incorporation de la société. La liste se trouve à l'adresse suivante : https://sectigo.com/

Deuxième étape : Le Client doit compléter et signer les deux documents suivants :

EV SSL Certificate Request Form - Simplified
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFOe

EV SSL Certificate Subscriber Agreement
https://comodoca.my.salesforce.com/sfc/p/#1N000002Ljih/a/1N000000gHyK/v9LCRR6EMgcShpdiZNQxBOv7uR.zhoSpEwalpPruRjs

Troisième étape : Vérifier l'existence physique du Client. Le Client doit apparaître sur l'une des pages suivantes : http://www.dnb.com/ http://www.hoovers.com/
UK - https://www.gov.uk/government/organisations/companies-house

Si le Client n'apparaît pas sur l'une des pages précédentes, son existence physique peut être vérifiée grace à une lettre signée par un comptable ou un avocat. Il doit s'agir de l'une des deux lettres suivantes :

Sample Legal Opinion Letter for EV
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFM8

Sample Accountant Letter for EV
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000X5oi

Quatrième étape : Cette étape ne concerne que les organisations dont la création est inférieure à trois ans. Il s'agit de vérifier l'existence opérationnelle de l'organisation. C'est à dire vérifier que cette dernière exerce réellement une activité. Le Client doit apparaître sur l'une des pages suivantes : http://www.dnb.com/
http://www.hoovers.com/

Si le Client n'apparaît pas sur l'une des pages précédentes, son existence opérationnelle peut être vérifiée grace à une lettre signée par un comptable ou un avocat. Il doit s'agir de l'une des deux lettres suivantes :

Sample Legal Opinion Letter for EV
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFM8

Sample Accountant Letter for EV
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000X5oi

Cinquième étape : Vérification du Whois associé.

Sixième étape : Vérification de l'existence du numéro de téléphone. Le Client doit apparaître sur l'une des pages suivantes :
http://www.scoot.co.uk/ http://www.192.com/ https://www.yell.com/
http://www.thephonebook.bt.com/publisha.content/en/search/business_by_name/search.publisha
http://www.118118.com/ http://www.dnb.com/
http://www.hoovers.com/

Les répertoires en ligne locaux peuvent aussi être utilisés.

Si le Client n'apparaît pas sur l'une des adresses précédentes, son numéro de téléphone peut être vérifié grace à une lettre signée par un comptable ou un avocat. Il doit s'agir de l'une des deux lettres suivantes :

Sample Legal Opinion Letter for EV
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFM8

Sample Accountant Letter for EV

https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000X5oi

Septième étape : Vérification téléphonique. Les personnes suivantes seront consultées par téléphone :

- Le demandeur du Certificat SSL
- Le signataire du Certificat SSL
- Le valideur du Certificat SSL
- Le signataire du « Subscriber Agreement »

Si ces personnes ne sont pas joignables, le service des ressources humaines sera alors consulté.

Une fois que tous les appels ont été faits l'équipe de validation EV procédera à une deuxième étape d'approbation, où chaque document sera vérifié pour vérifier qu'il se conforme aux directives EV.