

CONDITIONS PARTICULIERES DE VENTE CERTIFICATS SSL/TLS

SOMMAIRE

1. OBJET	2
2. DEFINITIONS.....	2
3. CONDITIONS DE FOURNITURE DU SERVICE	3
4. INTERFACE DE GESTION	3
5. OBLIGATIONS ET RESPONSABILITES DU CLIENT	3
5.1 Mandat donné à Ikoula	3
5.2 Processus de validation	3
5.3 Exactitude des informations transmises	4
5.4 Hébergement, autorisations et Clé Privée	4
5.5 Utilisation du Certificat SSL/TLS	4
6. OBLIGATIONS ET RESPONSABILITES D'IKOULA.....	4
6.1 Obligation de moyens et rôle d'intermédiaire	4
6.2 Responsabilité.....	5
7. DUREE	5
7.1 Durée Contractuelle.....	5
7.2 Durée de validité des Certificats SSL/TLS et réémissions	5
7.3 Procédure de réémission et rôle du Client	6
7.4 Renouvellement du Service	6
7.5 Résiliation et fin du Service.....	6
7.6 Révocation du Certificat SSL/TLS.....	7

1. Objet

Les présentes conditions particulières (ci-après les « **Conditions Particulières** ») ont pour objet de définir les conditions dans lesquelles Ikoula propose à son Client le Service de Certificat SSL/TLS dans le cas où le Client dispose d'un Nom de Domaine (ci-après le « **Service** »).

2. Définitions

- **Autorité de Certification** : entité de confiance en charge de la délivrance des Certificats SSL/TLS.
- **Certificat SSL/TLS (également appelé un « Certificat » ou « Certificat Électronique »)** : SSL est l'acronyme anglais de « Secure Socket Layer ». TLS est l'acronyme anglais de « Transport Layer Security ». Ces sigles désignent des protocoles standards de sécurisation de la transmission de données sur Internet. Le protocole TLS est le successeur moderne et sécurisé du protocole SSL. Dans les présentes Conditions Particulières, les termes « Certificat SSL/TLS », « Certificat » et « Certificat Électronique » désignent indifféremment un certificat SSL/TLS, quelle que soit l'Autorité de Certification qui l'a délivré. Un Certificat SSL/TLS 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/TLS 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** : fichier de données électronique chiffré 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** : fichier de données électronique chiffré et confidentiel conçu pour être en liaison avec une Clé Publique utilisant le même algorithme de chiffage et qui peut être utilisé pour créer des Signatures Numériques, pour déchiffrer des fichiers ou des messages qui ont été chiffrés avec une Clé Publique. La Clé Privée est au Client et Ikoula ne fournit pas les Clés Privées sauf si Ikoula a généré la CSR (Certificate Signing Request) concomitamment à la Clé Privée.
- **Clé Publique** : fichier de données électronique chiffré et librement disponible qui est conçu pour être en liaison avec une Clé Privée utilisant le même algorithme de chiffage et qui peut être utilisé pour vérifier les Signatures Numériques et pour chiffrer des fichiers ou des messages.
- **DNS (Domain Name System)** : service informatique distribué qui associe les Noms de Domaine avec leurs adresses IP ou d'autres types d'enregistrements. Dans le cadre du Service, la validation dite « DNS » consiste, pour le Client, à ajouter dans la zone DNS de son Nom de Domaine un enregistrement communiqué par l'Autorité de Certification, afin de démontrer qu'il contrôle ce Nom de Domaine.
- **Nom(s) de Domaine** : adresse littérale d'un site internet. Un Nom de Domaine de second niveau est composé d'un radical (exemple : « ikoula ») et d'une extension ou TLD (exemple « .com »), cette extension étant considérée comme un Nom de Domaine de premier niveau. Il est à noter qu'un Nom de Domaine peut être agrémenté d'un ou même plusieurs préfixes (exemple : « www »).

- **Serveur** : désigne le serveur du Client fonctionnant avec l'adresse IP identifiée par un Nom de Domaine par le Client à Ikoula et qui est lié de manière chiffrée à la Clé Publique présentée dans le Certificat SSL/TLS.

3. Conditions de fourniture du Service

Le Client reconnaît que le Certificat SSL/TLS 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'Ikoula ou d'un bureau d'enregistrement tiers, au cours ou au terme de son engagement contractuel.

S'agissant de la fourniture du Nom de Domaine, dans l'hypothèse où ce dernier serait fourni par Ikoula, le Client s'engage à prendre connaissance des conditions particulières afférentes.

4. Interface de gestion

Ikoula met à disposition du Client une interface de gestion (ci-après « **l'Interface** ») permettant au Client de gérer les actions à effectuer concernant son Certificat SSL/TLS.

Le Client se voit attribuer un Code d'Accès confidentiel pour accéder à l'Interface. Il s'engage à préserver la confidentialité de ce Code d'Accès et à ne pas le divulguer à des tiers non autorisés. Le Client est seul responsable de son Code d'Accès et de toute activité effectuée avec celui-ci sur l'Interface, y compris des conséquences qui peuvent en découler. Ainsi, tout acte effectué avec les identifiants du Client sera considéré comme réalisé par ce dernier.

Le Client notifiera immédiatement Ikoula en cas de perte, vol ou utilisation non autorisée de son Code d'Accès. Dans ce cas, Ikoula se réserve le droit de bloquer l'accès et de fournir de nouveaux identifiants.

Le Client est responsable de la sécurisation de l'accès à son compte sur l'Interface et s'engage à prendre toutes les mesures raisonnables pour empêcher tout accès non autorisé à son Code d'Accès ou à son compte.

L'utilisation par le Client de tout autre identifiant et mot de passe qui pourrait être transmis par Ikoula sera soumise aux mêmes règles, modalités et obligations que celles énoncées pour le Code d'Accès.

5. Obligations et responsabilités du Client

5.1 Mandat donné à Ikoula

Le Client mandate Ikoula pour agir en tant qu'intermédiaire auprès de l'Autorité de Certification notamment pour accepter, au nom et pour le compte du Client, 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 Ikoula à transmettre à l'Autorité de Certification toute information qui lui serait demandée dans le cadre strict de la fourniture du Service.

5.2 Processus de validation

L'Autorité de Certification procédera au processus de validation du Certificat SSL/TLS demandé par le Client. Le Client sera directement contacté par l'Autorité de Certification à ce titre.

Dans le cas où le Client choisit la validation DNS, et que le DNS n'est pas géré chez Ikoula, le Client devra impérativement contacter le support technique d'Ikoula afin de renseigner les champs nécessaires permettant la validation.

5.3 Exactitude des informations transmises

Le Client s'engage à communiquer à Ikoula, et à renseigner sur l'Interface, des coordonnées et informations de contact exactes, complètes et régulièrement mises à jour.

En cas de coordonnées ou d'informations incorrectes, incomplètes ou obsolètes, Ikoula ne peut garantir au Client la possibilité d'effectuer les opérations relatives au Certificat SSL/TLS, et le Certificat SSL/TLS est susceptible de faire l'objet d'un refus d'émission ou d'une révocation par Ikoula ou l'Autorité de Certification. Le Client décharge Ikoula de toute responsabilité à ce titre.

5.4 Hébergement, autorisations et Clé Privée

Le Client s'engage à être seul responsable de l'espace d'hébergement du site sur lequel est installé le Certificat Électronique 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/TLS 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.

5.5 Utilisation du Certificat SSL/TLS

Le Client ne devra pas utiliser le Certificat SSL/TLS 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 peindraient, 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/TLS raisonnablement, au sens des dispositions du Code civil mais également de la jurisprudence actuelle.

6. Obligations et responsabilités d'Ikoula

6.1 Obligation de moyens et rôle d'intermédiaire

Ikoula 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, dans le cadre d'une obligation de moyens.

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

6.2 Responsabilité

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

LE CLIENT RECONNAIT AUSSI QU'IKOULA 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.

7. Durée

7.1 Durée Contractuelle

Le Service est souscrit par le Client pour une durée d'un (1) an à cinq (5) ans à compter de la date d'émission du Certificat SSL/TLS (ci-après la « Durée Contractuelle »).

La Durée Contractuelle est indépendante de la durée de validité technique du Certificat SSL/TLS effectivement émis (ci-après la « Durée du Certificat SSL/TLS »).

7.2 Durée de validité des Certificats SSL/TLS et réémissions

En application des règles édictées par le CA/Browser Forum et par les Autorités de Certification, la Durée du Certificat SSL/TLS peut être inférieure à la Durée Contractuelle et est susceptible d'être progressivement réduite. Plusieurs Certificats SSL/TLS successifs pourront ainsi être émis au cours de la Durée Contractuelle, sans que cette circonstance ouvre droit à un quelconque remboursement ou indemnité au bénéfice du Client.

Pendant la Durée Contractuelle, Ikoula pourra procéder ou demander au Client de procéder à toute nouvelle émission, réémission ou opération de validation rendue nécessaire par les règles applicables aux Certificats SSL/TLS ou par l'Autorité de Certification. Ces opérations n'ont pas pour effet de prolonger la Durée Contractuelle et, comme les réémissions successives du Certificat SSL/TLS nécessaires pour couvrir la Durée Contractuelle, sont comprises dans le prix de la souscription et ne donnent lieu à aucune facturation complémentaire, sauf prestation distincte expressément commandée par le Client.

La réémission d'un Certificat SSL/TLS pendant la Durée Contractuelle ne proroge pas cette dernière, réémission du Certificat SSL/TLS et renouvellement contractuel du Service étant deux opérations distinctes.

Chaque Certificat SSL/TLS émis ou réémis a une Durée du Certificat SSL/TLS fixée par l'Autorité de Certification. Cette durée ne peut excéder la durée maximale autorisée par les règles applicables aux Certificats SSL/TLS, même lorsque la durée restant à courir de la Durée Contractuelle est plus longue. Plusieurs réémissions sont donc nécessaires pour couvrir l'intégralité de la Durée Contractuelle. La Durée du Certificat SSL/TLS n'a aucune incidence sur la date de fin de la Durée Contractuelle.

Lorsqu'une réémission intervient à l'approche du terme de la Durée Contractuelle, la Durée du Certificat SSL/TLS réémis est limitée à la durée restant à courir jusqu'à ce terme.

7.3 Procédure de réémission et rôle du Client

La réémission d'un Certificat SSL/TLS en cours de Durée Contractuelle se distingue du renouvellement du Service et ne nécessite aucune nouvelle commande. Ikoula informe le Client, par courrier électronique adressé soixante (60) jours, trente (30) jours puis quinze (15) jours avant l'expiration de la Durée du Certificat SSL/TLS en cours, de l'engagement prochain de la procédure de réémission. Les notifications relatives au Service sont adressées aux coordonnées renseignées par le Client dans son compte client sur l'Interface. Il appartient au Client de maintenir ces coordonnées à jour, conformément à l'article 5.3 des présentes.

La réémission du Certificat requiert la participation active du Client. Le Client s'engage à réaliser, dans les délais qui lui sont indiqués, les opérations nécessaires à l'émission ou à la réémission de son Certificat SSL/TLS, notamment les opérations de validation du domaine ou de l'organisation et, lorsque cela est requis, la fourniture des informations ou éléments techniques nécessaires. Il lui appartient également de récupérer le Certificat SSL/TLS réémis et de l'installer ou de le réinstaller sur son Serveur avant l'expiration du Certificat SSL/TLS en cours. Sauf souscription d'une prestation spécifique d'infogérance, Ikoula ne fournit pas d'assistance à ce titre.

À défaut de réponse du Client ou de réalisation des opérations lui incombant dans les délais requis, le Certificat SSL/TLS peut expirer ou ne pas pouvoir être émis ou réémis, entraînant une interruption de la protection HTTPS. L'absence de Certificat SSL/TLS valide résultant de cette carence ne constitue pas une indisponibilité imputable à Ikoula, la Durée Contractuelle continuant de courir, et n'ouvre droit à aucun remboursement ni indemnité.

7.4 Renouvellement du Service

Le renouvellement du Service à l'issue de la Durée Contractuelle nécessite une nouvelle commande, donnant lieu à une nouvelle facturation et à un nouveau processus de validation. Il fait courir une nouvelle Durée Contractuelle à compter de l'émission du premier Certificat SSL/TLS au titre de cette nouvelle commande.

Le paiement anticipé du renouvellement du Service, le cas échéant, n'a pas, à lui seul, d'incidence sur la Durée du Certificat SSL/TLS en cours. La nouvelle période de validité du Certificat SSL débute à compter du déclenchement effectif de la procédure de réémission du Certificat. Ainsi, lorsque le Client déclenche cette procédure avant l'expiration de la Durée du Certificat SSL/TLS en cours, les jours de validité restant sur ce dernier ne sont ni reportés ni ajoutés à la Durée du Certificat SSL/TLS renouvelé.

7.5 Résiliation et fin du Service

Le Service 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 quinze (15) jours 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.

En complément des dispositions des Conditions Générales de Vente ou du Contrat-cadre, le Client reconnaît et accepte que, dans l'hypothèse où l'Autorité de Certification ou tout autre fournisseur tiers mettrait fin aux contrats autorisant Ikoula à commercialiser ou à revendre les Certificats SSL/TLS, ou dans le cas où l'Autorité de Certification cesserait ses opérations ou ne disposerait plus du droit de délivrer des

Certificats SSL/TLS, Ikoula s'engage à en informer le Client dans les meilleurs délais et à mettre en œuvre, dans un délai de trente (30) jours suivant cette notification, toute solution de substitution permettant d'assurer la continuité du Service dans des conditions équivalentes.

Si, à l'issue de ce délai, aucune solution de substitution n'est disponible, Ikoula pourra résilier le Service moyennant un préavis de quinze (15) jours, notifié par écrit au Client. Dans ce cas, aucune indemnisation ne sera due au Client au titre de cette résiliation.

De même, si la solution de substitution proposée ne lui convient pas, le Client pourra résilier le Service moyennant un préavis de trente (30) jours.

Ikoula peut également résilier le Service avec effet immédiat en cas de motif légitime, notamment en cas de manquement grave du Client ou de violation par celui-ci des réglementations applicables ou des règles d'éthique.

La fin du Service, quelle qu'en soit la cause, met fin à toute obligation d'Ikoula au titre du Service, notamment à toute opération d'émission, de réémission, de validation, de renouvellement, d'assistance ou de notification relative au Certificat SSL/TLS.

7.6 Révocation du Certificat SSL/TLS

La révocation du Certificat se distingue de la résiliation du Service : elle est l'invalidation définitive d'un Certificat SSL/TLS avant sa date d'expiration, exécutée par l'Autorité de Certification.

Le Client peut demander à tout moment la révocation de son Certificat SSL/TLS.

Il doit la demander sans délai, et au plus tard dans les vingt-quatre (24) heures, en cas de compromission de sa Clé Privée ou si les informations figurant dans le Certificat SSL/TLS deviennent inexactes.

L'Autorité de Certification peut également révoquer un Certificat SSL/TLS dans les cas prévus par ses règles, notamment en cas de compromission de la Clé Privée, d'informations inexactes, de manquement du Client, d'usage illicite ou de perte du droit d'utiliser le Nom de Domaine.

Un Certificat SSL/TLS révoqué ne peut être réactivé. Sa réémission ou son remplacement relève de la seule appréciation de l'Autorité de Certification. Ikoula ne garantit aucunement la réémission ou le remplacement d'un Certificat SSL/TLS révoqué et ne saurait être tenue responsable d'un refus de l'Autorité de Certification.

Dès la révocation, le Client doit impérativement cesser toute utilisation du Certificat SSL/TLS révoqué et de la Clé Privée associée.

La révocation n'ouvre droit à aucun remboursement, sous réserve des dispositions impératives applicables.

L'Autorité de Certification pouvant révoquer un Certificat SSL/TLS selon ses propres règles, y compris sans motif, Ikoula ne saurait être tenue responsable d'une révocation décidée par l'Autorité de Certification, ni du délai de prise en compte d'une demande de révocation par celle-ci.