

Zone réservée à l'Autorité d'Enregistrement (AE)

Raison Sociale de l'Autorité d'Enregistrement: DKB Solutions



Le Service DKB SOLUTIONS est joignable du lundi au vendredi, de 9h à 18h, jours ouvrés, excepté jours fériés légaux. Le service clients de l'AE est directement accessible par email ou par téléphone aux coordonnées suivantes

Téléphone :	+225 22 47 00 50
Fax :	+225 22 47 04 75
e-mail :	info@dkbsolutions.com
Adresse Postale :	DKB Solutions Riviera 3 RUE E128 - 17BP 519 Abidjan 17 - Côte d'ivoire
E-mail Correspondant à la protection des données à caractères personnel :	myreille.cophey@dkbsolutions.com

Demande de Certificat SSL OV "OrganizationValidated"

Information relative au certificat

Durée de validité du certificat :

1 an

2 ans

3 ans

Type de requête :

Création

Renouvellement

Upgrade

Nombre de Licences

Nombre de SAN supplémentaires

CN: FQDN, Wildcard ou IP <i>Attention: cette valeur doit être identique à une seule des valeurs définie pour l'extension SAN ci-dessous</i>	
O : <i>Nom officiel complet de l'organisation cliente tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, ...) et tel qu'inscrit dans le tableau « INFORMATIONS de l'entité légale de l'ORGANISATION Propriétaire du nom de domaine » sur la ligne « N° d'immatriculation (RCS ou équivalent) »</i>	
OU: <i>numéro RCCM</i>	
L : <i>Ville d'implantation du siège de l'Organisation</i>	
C: <i>Code ISO Pays. Ce code est inscrit en majuscules sur 2 caractères</i>	

Demande de Certificat SSL OV "OrganizationValidated"

Attention, les clés RSA doivent avoir une longueur au moins égale à 2048 bits pour être acceptées.

CSR (base 64 avec balises BEGIN /
END) La CSR doit être format
texte ou Notepad.

Page à remplacer par l'impression papier de la CSR (base 64 avec balises BEGIN / END). La CSR doit être format texte ou Notepad.

Demande de Certificat SSL OV "OrganizationValidated"

SAN (le total des SAN Dns Name et IP définis ci-dessous ne doit pas dépasser 99 entrées)
Liste des SAN "Dns Name" - à insérer ci-dessous séparés par un point-virgule «;»
Liste des SAN "IP" - à insérer ci-dessous séparés par un point-virgule «;»

Demande de Certificat SSL OV "OrganizationValidated"

Information concernant le Contact Technique

Tous les champs doivent être remplis

Nom	
Prénom	
Fonction	
Organisation (si différent de l'organisation titulaire)	
Adresse email	
Téléphone direct	

Justificatif d'identité du Contact Technique

La copie de la Pièce d'identité doit être lisible afin de pouvoir vérifier les informations qui y sont portées. La pièce d'identité doit être valide.

Remarques : Pour une Carte Nationale d'Identité, utilisez un cadre pour le recto, un cadre pour le verso. Pour le passeport, utilisez un seul cadre.

**Page à remplacer par la photocopie de la pièce d'identité
du CT.**

Demande de Certificat SSL OV "OrganizationValidated"

Contact Technique

"J'atteste que toutes les informations fournies dans ce formulaire sont correctes.

J'atteste sur l'honneur l'exactitude et la véracité de tous les éléments que j'ai fournis dans ce formulaire et des pièces justificatives qui l'accompagnent. J'ai lu les conditions générales d'utilisation et les accepte sans réserve.

Date et Signature du Contact Technique

--

Autorité d'enregistrement AE

"J'atteste sur l'honneur avoir vérifié la complétude et la cohérence de ce dossier.

Nom, Prénom, Date et Signature de l'AE

--

CONDITIONS GENERALES D'UTILISATION

Objet :

Les présentes conditions générales de service ont pour objet de définir les conditions juridiques, techniques et financières de l'obtention des Certificats OV SSL par le Client ainsi que les conditions d'utilisation et les obligations respectives des Parties. **La signature de la demande de Certificat SSL OV par le Client (ci-après la "Commande") sera considérée comme étant l'acceptation inconditionnelle et irrévocable par le Client d'adhérer aux présentes conditions générales**, et comme une renonciation à ses propres conditions générales d'achat. Aucune Commande ne pourra être annulée ou modifiée.

Définitions :

Autorité de Certification (ou AC) :

Désigne l'une des composantes de l'Infrastructure de Clés Publiques (ICP) générant et distribuant des Certificats SSL, et ce en application des règles et des pratiques déterminées par elle dans sa Politique de Certification (PC). Dans le cadre des présentes, l'Autorité de Certification de DKB SOLUTIONS émettrice des Certificats SSL est dénommée "AC DKB Solutions MACHINES" qui est techniquement et hiérarchiquement rattachée à l'AC Racine indiquée dans la PC.

Autorité d'Enregistrement (ou AE) :

Désigné dans le formulaire, un des acteurs de l'IGC approuvé par l'AC et dont le rôle est de (i) identifier et authentifier le Contact Technique désigné dans la demande de certificat et son appartenance à l'entité légale telle que décrite dans la demande de certificat ainsi que l'existence légale de l'entité légale, (ii) enregistrer les demandes d'émission, de renouvellement et de révocation de Certificats, (iii) après validation d'une demande de Certificat, générer les Certificats OV SSL, (iv) transmettre les Certificats et la chaîne de confiance d'AC permettant de valider les Certificats par courrier électronique au Contact Technique, (v) adresser les Codes de révocations par courrier électronique au Contact Technique et (vi) révoquer sur demande authentifiée les Certificats OV SSL. L'AE applique des procédures d'identification et d'authentification conformément aux règles de la Politique de Certification, de la DPC associée et des procédures de gestion de certificats validées par l'AC. Dans le cadre de l'émission d'un Certificat OV SSL, l'AE valide uniquement que le Contact Technique est autorisé à gérer le FQDN, le Wildcard et/ou l'adresse IP demandée par le Client en utilisant entre autre le service WHOIS d'un ou de plusieurs Registrar et que l'entité légale existe officiellement et que le Contact Technique appartient par l'entité légale.

Certificat OV SSL :

Désigne un certificat électronique « OrganizationValidated (OV) » ayant pour objet de permettre la mise en place d'une connexion SSL/TLS "Secure Socket Layer" sécurisée entre un serveur de site web disposant du Certificat SSL et le Client se connectant au site web (key usages : digital signature et key encipherment). Un Certificat OV SSL contient l'information sur l'organisation qui possède l'IP, le Wildcard ou le FQDN contenu dans le Certificat OV SSL. Les certificats sont émis conformément aux exigences du CAB Forum (<https://www.cabforum.org>) et de l'ETSI 102 042 (OVCP).

Chemin de certification (ou chaîne de confiance, ou chaîne de certification) : désigne l'ensemble d'AC où chaque AC est certifiée par une AC d'échelon supérieur. À titre d'illustration, une AC délivrant des certificats à des Contact Techniques peut elle-même être certifiée par une AC, dite « AC intermédiaire », qui à son tour peut être certifiée par une autre AC intermédiaire, ainsi de suite jusqu'à l'AC de plus haut niveau, auto signée, dite « AC racine ».

Client : désigne l'entité qui réalise auprès de l'AE une demande de Certificat SSL dans le cadre de son activité professionnelle et qui contracte avec l'AE. Le Client désigne une personne (Contact Technique) en charge des opérations suivantes :

- Génère la bi-clé et la CSR à faire certifier par l'AC ;
- Elabore et signe la demande de certificat ;
- Récupère le certificat OV SSL ;
- Gère la révocation du certificat OV SSL.

Code de révocation : désigne le code défini par l'AE et adressé par l'AE au Client par courrier électronique lui permettant de révoquer seul son Certificat sur l'URL de révocation adressée aussi au Client par courrier électronique.

Contrat : désigne l'ensemble contractuel constitué des présentes conditions générales, du formulaire de

Demande de Certificat SSL OV "OrganizationValidated"

demande de Certificat, ainsi que les procédures applicables figurant sur le site web de l'AE, applicables à la date de demande de Certificat par le Client.

Espace de Nom de domaine : L'ensemble de tous les noms possibles de domaine qui sont subordonnées à un nœud unique dans le système des noms de domaine.

Fully-Qualified Domain Name (FQDN) : un Nom de domaine qui comprend les étiquettes de tous les nœuds supérieurs dans le système des noms de domaine de l'Internet.

Nom de domaine : Le label attribué à un nœud dans le système des noms de domaine.

Politique de Certification : désigne l'ensemble de règles énoncées 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, des Clients et Utilisateur de Certificat et de toutes les composantes de l'IGC intervenant dans l'ensemble du cycle de vie d'un Certificat OV SSL. Dans le cadre des présentes, la Politique de Certification (PC) applicable consultable à l'adresse web suivante : <https://dkbsolutions.com/fr/pki> Dont l'OID est 1.3.6.1.4.1.46111.1.3.101.11.

Registrar : Une entité légale qui enregistre et gère officiellement des noms de domaine en conformité avec les règles de l'ICANN (Internet Corporation for Assigned Names and Numbers). Un Registrar met en œuvre un service dit « WHOIS » de recherche d'information sur la gestion des Noms de domaine (y compris pour les Wildcard) et les adresse IP vérifiables sur internet.

Utilisateur du Certificat : désigne la personne physique ou morale qui fait confiance aux Certificats OV SSL, pour ses relations commerciales avec l'entité dont le(s) nom(s) de domaine est (sont) inclus dans le certificat SSL.

Wildcard : Un nom de domaine complet contenant un astérisque (*) dans la position la plus à gauche dans le FQDN Client.

3. Description du service de certification OV SSL

Les conditions d'utilisation du service de certification électronique "SSL OV" (Service) sont décrites et régies par la Politique de Certification de l'Autorité de Certification (ci-après dénommée "Politique de Certification") régulièrement modifiée et amendée, laquelle fait partie intégrante du présent accord.

En acceptant les présentes conditions générales, le Client reconnaît avoir pris connaissance et être lié par les termes de la Politique de Certification Le Certificat SSL a une durée de validité d'un (1), deux (2), 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. Suite à la signature de la demande de certificat par le Contact Technique et l'acceptation de la demande de certificat par l'AE, l'AE génère le Certificat OV SSL et transmet par courrier électronique le certificat et la chaîne de confiance au Contact Technique.

4. Procédure de demande de Certificat

Le Contact Technique effectuera une Demande de Certificat selon la procédure communiquée par l'AE auprès du Contact Technique. Le CT récupère la clé publique à mettre dans le Certificat OV SSL et l'insère dans le Formulaire de demande ainsi que l'ensemble des pièces justificatives requises par l'AE. Le Formulaire de demande de certificat, au format papier, est daté et signé par le Contact Technique, qui en paraphe chacune des pages, suivant la procédure indiquée par l'AE. Le CT transmet cette demande dûment complétée à l'AE soit directement auprès de l'AE soit par courrier postal.

5. Traitement des demandes de certificat SSL OV

A réception de la demande d'un Certificat SSL OV effectuée par un Contact Technique, l'AE procède à la vérification des informations et pièces fournies par le Contact Technique. En outre, l'AE vérifie la bonne réception de la Commande et de son complet paiement. Lors de la demande, le Contact Technique 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 l'AE et accompagnée de justificatifs requis. En tout état de cause, le Contact Technique est informé qu'en cas de dossier incomplet, ou dans l'hypothèse où le Contact Technique n'aurait pas communiqué à l'AE les informations nécessaires demandées, l'AE en informe le Client et le Contact Technique. La demande de Certificat SSL OV sera alors mise

Demande de Certificat SSL OV "OrganizationValidated"

en attente par l'AE jusqu'à complétude du dossier. En tout état de cause, le Certificat SSL OV ne sera délivré au Contact Technique qu'à réception du complet paiement de la Commande. Suite à la génération du Certificat, le Code de révocation défini par l'AE, est adressé par l'AE au Contact Technique par courrier électronique qui contient donc le Code de révocation et l'URL à utiliser pour accéder à l'interface web de révocation en ligne de l'AE. Après avoir récupéré et installé son Certificat, le Contact Technique devra en contrôler le contenu et informer l'AE de toute erreur qu'il aurait détectée. Dans ce cas, l'AE révoquera ledit Certificat et émettra un nouveau Certificat corrigé. Une fois que le Contact Technique a récupéré et installé son certificat, le Contact Technique doit examiner, sous un délai de 15 jours, et vérifier le contenu du certificat et informer l'AE si des erreurs sont détectées. Dans ce cas, l'AE révoque ledit certificat et délivre un nouveau certificat rectifié. Passer le délai de 15 jours, le certificat est considéré comme accepté par l'AE et l'AC.

Toutefois, le CT, le Représentant Habilité et le MC reconnaissent et acceptent :

- Les caractéristiques et les limites concernant la transmission par voie de courrier électronique des Codes de révocation, notamment en termes de délai de délivrance, d'utilisation frauduleuse, de perte, d'interception, ou de vol des courriers électroniques ;
- En particulier, que la communication par Internet de mots de passe et codes confidentiels n'est pas exempte de tout risque, et qu'ils doivent prendre toutes les mesures appropriées de façon à protéger leurs 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 ;
- Avoir connaissance des limites quant au délai de délivrance pour recevoir des courriers postaux.

6. Renouvellement d'un Certificat

Le renouvellement d'un Certificat SSL OV implique la génération d'un nouveau Certificat, se fait suivant la même procédure qu'une demande initiale de Certificat. Le CT doit utiliser une nouvelle bi-clé pour obtenir un nouveau Certificat OV SSL.

7. Révocation d'un Certificat

Le Certificat SSL OV peut être révoqué lorsque le lien entre ce dernier et la clé publique associée n'est plus valable. Le Contact Technique devra avertir sans délai l'AE 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, du Wildcard ou de l'IP.

L'AE 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.

Seules les révocations qui sont effectuées sur l'interface web (dont l'URL est fournie au Contact Technique par courrier électronique) en utilisant le code de révocation (qui est fourni au Contact Technique par courrier électronique) sont prises en compte en 24H00. Si le Contact Technique procède une demande de révocation auprès de l'AE en passant par un autre moyen, alors la demande de révocation est prise en compte dans les meilleurs délais durant les heures ouvrées de l'AE. Le Contact Technique est également informé qu'en cas d'expiration ou résiliation du contrat de Service conclu entre l'AE et l'AC, quelle qu'en soit la cause, il pourra révoquer son Certificat sur le site web de l'AE à l'aide de son Code de révocation. Il est en outre du ressort de l'AE d'avertir l'Utilisateur d'une telle rupture contractuelle.

8. Durée du Contrat

Le présent Contrat prend effet à la date de commande du Certificat 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 ou de l'AE, l'AE et l'AC se réservent le droit de révoquer sans délai son Certificat.

Demande de Certificat SSL OV "OrganizationValidated"

9. Conditions financières

Le prix du Certificat applicable est celui mentionné dans l'offre communiquée par l'AE à la date de souscription ou du renouvellement dudit Certificat. Les conditions tarifaires du Certificat dépendent de leur durée de validité et du type de Certificat et de la licence choisi par le Client. A l'issue de la réception par l'AE de la demande de Certificat par le Client, une facture sera adressée par courriel ou par écrit papier au Client. La facture est payable par virement, par espèce ou par chèque. A réception du paiement du Client, l'AE procèdera à la délivrance du Certificat. En cas de dossier d'inscription incomplet rendant impossible la délivrance du Certificat commandé, l'AE 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 l'AE par lettre recommandée avec AR dans un délai d'un mois à compter de la date de commande, l'intégralité du montant versé restera acquise à l'AE à titre d'astreinte.

10. Restrictions d'usage

Le Client s'engage à n'utiliser les Certificats qui lui sont délivrés qu'en son nom propre et que pour les noms de domaines déclarés auprès de l'AE. 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, IP wildcard autre que celui qu'il a déclaré dans sa demande de certificat ("Common Name" et "Subject Alternative Name"). Le Client s'interdit d'utiliser la clé privée associée au Certificat 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.

11. Engagements du Client

Le Client s'engage à suivre les étapes de demande de Certificat, comme indiqué par l'AE, et à transmettre à l'AE 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 la clé privée associée au Certificat et le Certificat et tous les autres services de l'Autorité de Certification qui les délivre conformément aux dispositions de la Politique de Certification et aux présentes. Au cas où le Nom de domaine enregistré dans le Certificat ou l'organisation du Client changerait, le Client doit sans délai en informer l'AE par écrit qui révoquera alors le Certificat concerné et le Client s'engage à ne plus utiliser le Certificat concerné.

Le Client s'engage à répondre aux instructions de l'AE concernant la compromission des clés ou une mauvaise utilisation du certificat dans une période de temps spécifiée comme indiqué dans CP. Le Client accepte que l'AC et l'AE sont en droit de révoquer le certificat immédiatement si le requérant devait violer les termes des présentes conditions générales de service ou si l'AC ou l'AE découvre que le certificat est utilisé pour permettre à des activités criminelles telles que les attaques de phishing, la fraude, ou la distribution de logiciels malveillants. Le Client s'engage à prendre toutes les mesures propres à assurer la sécurité du ou des serveur(s) où est installée la clé privée associée au Certificat, et à prendre toutes dispositions nécessaires à la sauvegarde, si une sauvegarde est utilisée, sécurisée de la clé privée associée au Certificat. 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. Le Client garantit que seules des personnes autorisées sont en possession de sa clé privée et de son mot de passe 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 quelque moyen que ce soit, de la Clé privée et de son Certificat. Le Client s'engage à cesser sans délai l'utilisation du certificat et de sa clé privée associée, et fait procéder sans tarder à la révocation du Certificat, dans le cas où : (i) toutes ou parties des informations dans le certificat est, ou deviennent, erronées ou inexactes, ou (ii) la clé est compromise ou suspectée de compromission. Suite à l'expiration ou à la notification de la révocation du Certificat du Client, le Client s'engage à définitivement retirer et détruire la clé privée associée au Certificat du ou des serveur(s) sur lequel ou lesquels elle est installée et ne doit plus utiliser cette clé quelle qu'en soit la raison. La destruction de la ou des clés copiées de clés privées doit garantir qu'elle ne puisse pas être réutilisées.

12. Engagements de l'AE et de l'AC

L'AC s'engage à maintenir, et ce pendant toute la durée de réalisation des prestations prévues, tous les moyens matériels et

Demande de Certificat SSL OV "OrganizationValidated"

humains lui permettant de conserver son référencement délivré par l'ARTCI pour l'AC et ce type de Certificat.

L'AE désignée dans le Formulaire de demande met à la disposition du Client des interfaces web de gestion des demandes de révocation de certificats.

L'AE 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. L'AE est tenue à une obligation de moyen pour les prestations prévues aux présentes.

L'AE est mis à disposition des Contact Techniques et traitera les questions relatives à l'obtention et l'utilisation du Certificat.

Les horaires d'ouverture et les coordonnées de l'AE sont communiqués au début du présent formulaire.

L'AE fournira au Contact Technique et au Client, le cas échéant, une prestation de suivi des incidents de service en fonction de sa commande, étant précisé que les incidents de service s'entendent uniquement sur les fonctionnalités de révocation en ligne des Certificats et d'installation du certificat. En ce qui concerne les questions relatives au fonctionnement des Certificat, l'AE est le seul contact du Contact Technique.

13. Responsabilité

13.1 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 l'AE et l'AC contre toute réclamation ou action, d'un tiers invoquant :

- Un manquement à l'un de ses engagements contractuels, notamment spécifiés à l'article 11 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 l'AE ;
- 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.

13.2 Responsabilité de l'AC et de l'AE

L'AC et l'AE ne sont 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. L'AC et l'AE ne garantissent 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 l'AC et de l'AE de toute utilisation non autorisée du Certificat et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée. L'AC et l'AE n'assument 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 ou téléphonique. En outre, l'AC et l'AE ne sont pas responsables de la qualité de la liaison internet et téléphonique du Client et du Contact Technique. Dans le cas où la responsabilité de l'AC et/ou de l'AE serait retenue au titre des présentes Conditions Générales d'Utilisation, il est expressément convenu que l'AC serait tenue à réparation des dommages directs certains et immédiats, dont le Client apportera la preuve, dans la limite de trois millions de francs CFA (3 000 000CFA), tous faits générateurs confondus. En outre, l'AC et l'AE excluent toute responsabilité en cas de non-respect par le Client de ses obligations définies dans les présentes et dans la Politique de Certification. L'AC et l'AE ne seront 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 l'AC et enregistré par l'AE. 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.

14. 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 l'AC et l'AE telles que définies aux présentes, sans que la responsabilité de l'AC et l'AE 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 et lois ivoiriennes, 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.

15. Protection des données à caractère personnel

Les données à caractère personnel recueillies auprès des Contact Techniques lors d'une Demande de Certificat font l'objet d'un traitement informatique par l'AE et l'AC, aux seules fins de permettre (i) leur authentification et leur identification par l'AE (ii) la réalisation des vérifications nécessaires à la délivrance d'un Certificat et le cas échéant à sa révocation, et (iii) le cas échéant la construction de leur identité portée dans le Certificat. Conformément à la loi ivoirienne (loi n°2013-450 du 19 juin 2013), les personnes concernées par le traitement bénéficieront du droit de demander la rectification de leurs informations personnelles dans la Demande de Certificat, et/ou de s'opposer à leur conservation en s'adressant en premier lieu au service client de l'AE (coordonnées dans le Formulaire de demande), et en cas de questions complémentaires au Correspondant à la protection des données à caractères personnel par e-mail, soit par courrier à l'adresse postale indiquée dans le Formulaire de demande. Il est rappelé que toute opposition à la conservation des données personnelles empêchera la délivrance du Certificat.

L'ensemble des données personnelles recueillies sont uniquement celles contenues dans le Formulaire de demande de certificat remis à l'AE. L'AE transmet par courrier électronique un scanne du Formulaire de demande de certificat au CT.

Les destinataires des données personnelles concernant les Contact Techniques sont le personnel de l'AE et de l'AC. Le correspondant à la protection des données à caractère personnelles pour l'AE est indiqué dans le Formulaire de demande et la PC. Les données personnelles sont conservées 7 ans après l'expiration du Certificat.

Une demande d'accès peut également être initiée sur demande judiciaire dans le cadre légal et réglementaire défini pour la Côte d'Ivoire. Le Porteur n'est pas forcément informé de ce type d'accès en fonction du besoin du demandeur. Dans ce cas, c'est l'AE et le responsable sécurité de l'AC qui authentifie ce type de demande.

16. Propriété intellectuelle

L'AC et l'AE 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 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. 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 dix (10) années suivant l'expiration ou la résiliation de celui-ci. De même, constituent des Informations Confidentielles les clés privées associées aux Certificats du Client, les mots de passes de protection et d'activation des clés privées associées aux Certificats du Client, les Codes de révocation, les secrets de l'IGC, les journaux d'événements des composantes de l'IGC, les dossiers d'enregistrement des Clients, et les

Demande de Certificat SSL OV "OrganizationValidated"

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

18. Dispositions diverses

18.1 Communication

Le Client autorise l'AC et l'AE 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.

18.2 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 l'AC et l'AE 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 l'AC et de l'AE découlant dudit Contrat seront transmis automatiquement au successeur sans qu'il soit nécessaire pour l'AC et l'AE de recueillir l'accord de la part du Client.

18.3 Assurance

L'AC et l'AE attestent avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations relatives au présent Contrat.

18.4 Convention de preuve

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 (Codes de révocation), Formulaire de demande de certificat et 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 échangés, et acceptés par l'AE, 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.

18.5 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.

18.6 Notifications Toute notification adressée au titre des CGU 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 d'un (1) mois suivant la survenance de l'événement motivant ladite réclamation.

19. 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 d'Abidjan, 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

Demande de Certificat SSL OV "OrganizationValidated"

sur injonction de payer.