

CONDITIONS GENERALES D'UTILISATION

1 Objet

Les présentes Conditions Générales d'Utilisation (ci-après « Conditions Générales » ou CGU) ont pour objet de définir les conditions juridiques relatives à l'obtention et l'utilisation des Certificats de signature et d'authentification de l'AC, de l'AE, du CT, du Représentant Habilité de l'Entité légale du CT ou le cas échéant du Mandataire de Certification.

2 Définitions

Autorité de Certification (ou AC) : désigne l'un des acteurs de l'Infrastructure de Gestion de Clés (IGC) générant des Certificats et assurant la gestion de leur cycle de vie, sur demande de l'Autorité d'Enregistrement, et ce en application des règles déterminées dans sa Politique de Certification (PC) et les pratiques déterminées dans sa Déclaration des Pratiques de Certification (DPC) associée. Dans le cadre des présentes, l'Autorité de Certification émettrice des Certificats est identifiée dans ce formulaire. DKB SOLUTIONS est AC. L'AC utilisée est l'AC « AC DKB SOLUTIONS PERSONNES ».

Autorité d'Enregistrement (ou AE) : désignée dans le formulaire de demande, un des acteurs de l'IGC approuvé par l'AC et dont le rôle est de (i) identifier et authentifier le demandeur de Certificat ou CT, l'Entité légale du CT, ou le cas échéant le Mandataire de certification désigné par cette dernière, (ii) enregistrer les demandes d'émission, de renouvellement et de révocation de Certificats qui ont été préalablement vérifiées par l'AE avant de lui être transmises, et les valider ou les rejeter, (iii) après validation d'une demande de Certificat, personnaliser les Supports en générant des bi-clés, charger sur les Supports le(s) Certificat(s) émis et générer les codes PIN associés auxdits Supports, (iv) remettre les Supports aux CT, au MC et (v) adresser les Codes PIN aux CT. DKB SOLUTIONS est AE.

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 définies par l'AC.

Certificat : désigne un fichier électronique attestant du lien entre une Identité cachet serveur et la Clé publique associée à la clé privée contenue dans le Support. Le Certificat est signé électroniquement par l'AC. L'AE procède au chargement du Certificat sur le Support, lequel est ensuite remis en face-à-face par l'Opérateur central d'AE au CT ou le cas échéant par le MC au CT.

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 CT 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 ».

Code d'activation : désigne(nt) des valeurs de données qui sont nécessaires pour mettre en œuvre la Bi-clé à l'aide d'un logiciel choisi par le CT. Le Code d'activation (ou code PIN) est adressé par l'AE à le CT par courrier électronique, SMS ou par courrier sécurisé et devra impérativement être modifié par le CT avant toute utilisation.

Code de révocation : désigne(nt) le code défini et adressé par l'AE au CT, ainsi qu'au Représentant Habilité (ou MC) et l'AE, par courrier électronique aux adresses mail indiquées dans le Formulaire de Demande de Certificat, permettant ainsi au CT et au Représentant Habilité (ou MC) de révoquer seul son Certificat sur l'URL de révocation sur l'interface du logiciel d'AE.

Déclaration des pratiques de certification (DPC) : désigne l'énoncé des pratiques que l'AC, utilise pour approuver ou rejeter les demandes de Certificats (émission, renouvellement et révocation), étant précisé que la DPC n'est pas un document public.

Demande de Certificat : désigne(nt) toute demande d'émission ou de renouvellement de Certificats effectuée par le CT sur le Formulaire prévu à cet effet. Chaque Demande est signée par le CT ainsi que, le cas échéant, le Représentant Habilité de l'Entité légale du CT ou le Mandataire de certification désigné.

Entité Légale : désigne la personne morale indiquée dans la Demande de Certificat, à laquelle le CT est rattachée, et au nom de laquelle ce dernier utilise les Certificats électroniques au moyen de son Identité Professionnelle.

Formulaire(s) : désigne(nt) les ou l'ensemble des formulaires fournis par l'AE et nécessaire à la gestion des Certificats.

Identité Cachet serveur : désigne l'identité construite à partir des informations recueillies par l'AE auprès du CT et celles définies par l'AC. Cette identité est utilisée pour authentifier un service applicatif d'une entité légale.

Kit Certificat : désigne collectivement l'ensemble remis au CT composé (i) du Support contenant tous les Certificats d'AC nécessaires à la validation du Certificat du CT, la bi-clé du CT et le Certificat associé, (ii) d'un Code d'activation pour utiliser le Support, (iii) de la documentation d'utilisation du Certificat et du Support et (iv) d'un Code de révocation permettant de révoquer en ligne le Certificat et une URL de service de révocation.

Mandataire de Certification (MC) : désigne une personne physique mandatée par l'Entité Légale du CT (i) pour procéder, au nom et pour le compte

de ce dernier, aux demandes de certificats auprès de l'AE, et (ii) pour se voir remettre, au nom et pour le compte du CT, les Supports de bi-clés. Le recours à un mandataire de certification (MC) n'est pas obligatoire.

Politique de Certification : désigne l'ensemble des règles énoncées par l'AC et publiées sur le site Internet de l'AC, décrivant les caractéristiques générales des Certificats qu'elles délivrent. Ce document décrit également les obligations et responsabilités de l'AC, de l'AE, des CT et de toutes les composantes de l'IGC intervenant dans l'ensemble du cycle de vie d'un Certificat. Dans le cadre des présentes, le CT devra respecter les règles décrites dans la Politique de Certification (PC) dont l'OID est défini dans le formulaire, applicable au Service est consultable à l'adresse web suivante : <https://dkbsolutions.com/fr/pki> dont l'OID est 1.3.6.1.4.1.46111.1.2.101.12.

Parties ou Partie : désigne ensemble ou individuellement l'AC, l'AE, les Opérateurs Centraux AE, le Représentant Habilité, le Mandataire de Certification et le CT ayant signé les présentes Conditions Générales.

CT : Désigne la personne physique gestionnaire d'un Certificat agissant pour le compte d'entreprises ou d'administrations. Le CT met en œuvre une Clé privée, à l'aide d'un Code PIN, correspondant à la clé publique certifiée par l'AC afin de signer des messages et des documents électroniques. L'identification et l'authentification d'un CT sont effectuées par l'AE. Le CT s'engage à respecter les conditions d'utilisation du Certificat et ses obligations vis-à-vis de l'AE telles que définies dans la Politique de certification de l'AC et dans les présentes Conditions Générales. A ce titre, le CT agit en tant que RCC (Responsables de certificats de cachets) au sens du RGS.

Procédures de gestion des Certificats : désigne l'ensemble des procédures édictées par l'AE que doivent respecter les CT, les Entités Légales via leurs Représentants Habilités ou via les MC qu'elles désignent, pour l'enregistrement, le renouvellement et la révocation des Certificats. En outre, le CT doit compléter le Formulaire de demande, accompagné des pièces justificatives nécessaires, afin de permettre à l'AE de vérifier les informations demandées par l'AC pour l'émission, le renouvellement ou la révocation d'un Certificat.

Renouvellement (d'un Certificat) : désigne l'opération effectuée en fin de période de validité d'un Certificat qui consiste à générer un nouveau Certificat pour un CT.

Représentant Habilité : désigne toute personne physique disposant des pouvoirs de représenter l'Entité Légale du CT de par la loi. Elle aura la faculté de procéder à des demandes d'émission, de renouvellement et de révocation de Certificat auprès de l'AE au bénéfice des CT qu'elle aura expressément et personnellement désignés. Dans la PC, le Représentant Habilité est appelé « Représentant Légal ».

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

Service : désigne l'ensemble des prestations fournies par l'AC, s'appuyant sur le Service AE de l'AC, pour permettre l'utilisation de Certificats et de bi-clé protégée par un code d'activation, incluant la mise à disposition d'un Portail d'AE pour la révocation en ligne.

Services associés : désigne le Service d'horodatage et le Service d'OSCP mis à disposition par l'AC et nécessaires pour l'utilisation des Certificats.

Service d'horodatage : désigne l'ensemble des prestations réalisées par l'AC nécessaires à la génération de contremarques de temps (ou jetons d'horodatage) en application de la Politique d'horodatage consultable à l'adresse web suivante : <https://dkbsolutions.com/fr/pki> . Cette contremarque de temps a pour objet de positionner dans le temps la réalisation et l'acceptation de la Transaction conclue en ligne par l'intermédiaire du Service.

Service d'OCSP (Online CertificateStatus Protocol) : désigne le service de vérification de l'AC mis à la disposition pour contrôler la validité des Certificats émis.

Support : désigne un support physique contenant un ensemble de composants logiciels utilisés pour mettre en œuvre la Clé privée et permettre des opérations cryptographiques (signature, vérification de signature et génération de bi-clé). Dans le cadre des présentes, le Support est une ressource cryptographique matérielle évaluée et certifiée EAL4+ et qualifiée renforcée suivant le schéma de qualification de l'ANSSI.

URL de révocation : désigne l'adresse du Site Internet de l'AC qui permet à un CT de révoquer son Certificat en saisissant le Code de révocation qui lui est associé.

Validation de Certificat électronique : Désigne l'opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le Certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La Validation d'un Certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaîne de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le Chemin de certification.

3 Procédure de demande de Certificat

Le CT et le Représentant Habilité (ou le MC s'il en est désigné un), effectueront une Demande de Certificat suivant les instructions communiquées par l'AE.

Tout Formulaire de demande de certificat devra être signé par le CT ainsi que par le Représentant Habilité de l'Entité Légale du CT suivant la

procédure indiquée ci-après au présent article.

En outre, lorsqu'un MC est expressément désigné par le Représentant Habilité, un Formulaire de création de mandat de MC devra être cosigné par le MC et le Représentant Habilité de l'Entité Légale. Un formulaire de demande de certificat pourra ensuite être complété et signé par le MC au nom de l'Entité Légale, ainsi que le CT. Le Formulaire de création de Mandat permettra au MC d'effectuer toute demande de Certificat et de révocation au nom de l'Entité Légale à compter de la date de signature dudit Formulaire.

Dès que le CT et le Représentant Habilité (ou le MC, s'il en est désigné un) ont dûment rempli le Formulaire de Demande de Certificat, le Formulaire et les informations de contacts du CT et du Représentant Habilité ou le cas échéant du MC s'il en est désigné un (nom, prénom, numéro de téléphone et courrier électronique) sont transmis à l'AE.

4 DELIVRANCE DU CERTIFICAT, DU SUPPORT, DU CODE DE REVOCATION ET DU CODE D'ACTIVATION

La remise du Certificat au CT, dans son Support, s'effectue lors d'un face-à-face avec l'AE. Dans le cas où le CT aurait mandaté un MC, l'identification et l'authentification du CT s'effectueront lors d'un face-à-face avec le MC. En tout état de cause, le CT, ou le cas échéant le MC, doit préalablement s'authentifier auprès de l'entité qui lui délivre le Certificat dans son Support en lui présentant une pièce d'identité officielle (carte nationale d'identité, passeport, etc.), identique à celle communiquée lors de la demande de Certificat, le cas échéant à celle communiquée dans le mandat de MC lorsqu'un MC est désigné. La remise du support par l'AE s'accompagne de la signature d'un bordereau de remise de Support qui est signé par la personne qui reçoit le Support et l'AE.

Parallèlement à la remise du Support au CT, l'AE adressera :

- Le Code d'activation soit ; par courrier électronique à l'adresse de courrier électronique, par SMS au numéro de téléphone ou par courrier sécurisé à l'adresse physique au CT indiquée sur le Formulaire de Demande de Certificat ;
- Le Code de révocation au CT et au Représentant Habilité (ou le cas échéant au MC) aux adresses de courrier électronique indiquées sur le Formulaire de demande de certificat.

Il est précisé que, pour des raisons de sécurité, l'envoi du Support et l'envoi du Code d'activation sont séparés dans le temps d'une durée de vingt-quatre (24) heures au minimum.

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 d'activation et 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 ;
- Que la communication par courrier postal de codes d'activation, et d'une manière générale, toute information confidentielle, est fait en connaissance de cause (utilisation par l'AC d'enveloppes sécurisées dont l'ouverture est détectable) ;
- Que des envois postaux peuvent être perdus, interceptés ou volés, en conséquence de quoi l'AC ne peut en aucun cas être tenue responsable d'une perte, d'un vol ou d'une interception de courriers.

A défaut de réception du Code d'activation alors même que le Support a été reçu, le CT et le Représentant Habilité ou le MC le cas échéant alerte à l'AE le plus vite possible.

Après réception du Support et du Code d'activation, il appartient à chaque CT de vérifier le contenu de son Certificat (dont principalement le champ « objet » du Certificat qui contient l'Identité Cachet serveur). Le CT disposera d'un délai de quinze (15) jours calendaires à compter de la réception du Support et du Code d'activation pour opposer son refus au contenu du Certificat et le transmettre à l'AE. Passé ce délai, le Certificat sera considéré comme accepté par le CT.

Le CT a l'obligation de changer son Code d'activation dès réception de celui-ci et de sa Bi-clé et ce, avant toute utilisation de sa Bi-clé dans le cadre d'un service en ligne.

5 Modalités d'utilisation du Certificat

Le CT doit prendre toutes mesures nécessaires afin de protéger sa Clé privée. Les utilisations de Certificats émis par l'AC à d'autres fins que celles prévues au présent article et dans la Politique de Certification ne sont pas autorisées. Dans le cas contraire, la responsabilité du CT pourrait être engagée. Le CT assure avoir pris connaissance, préalablement à la signature des présentes, de la documentation disponible, incluant les prérequis techniques, concernant le Certificat ainsi que des spécificités techniques pour l'utilisation dudit Certificat. Il appartient au CT de s'assurer que les matériels dont il dispose, notamment les logiciels de signature, sont susceptibles d'être utilisés avec toute l'efficacité requise avec le Certificat. La clé

privée associée au Certificat ne peut servir qu'à des fins de signature de document ou message électronique.

6 Durée de vie des Certificats

Le Certificat a une durée de validité de 3 (trois) ans maximum. Cette durée débute à compter de sa date d'émission par l'Autorité de Certification. A l'issue de cette période de validité du Certificat, la vérification de la signature des documents sera réalisable avec les logiciels de vérification indiqués par les entités qui déploient les applications utilisatrices du Certificat, notamment pour vérifier qu'à sa date de signature le document a été signé électroniquement par un Certificat valide émis par l'AC. Il est indiqué à ce titre qu'un Certificat expiré n'est plus contenu dans les CRL produites par l'AC et ce quel que soit son statut.

7 Renouvellement de Certificat

Lorsque la validité du Certificat aura expiré, le CT pourra renouveler le Certificat en effectuant une nouvelle Demande de Certificat auprès de l'AE conformément à la procédure qui lui sera indiquée. Un nouveau Kit Certificat est distribué au CT. Le renouvellement d'un Certificat implique la génération d'un nouveau Certificat, se fait suivant la même procédure qu'une demande initiale de Certificat.

8 Modalités de Révocation du Certificat

8.1 Révocation à l'initiative du CT

L'AE devra être avertie sans délai de toute demande de révocation de Certificat à l'initiative du CT ou du Représentant Habilité (ou le cas échéant du MC s'il en est désigné un).

Une demande de révocation du Certificat devra être effectuée dans les cas suivants :

- Les informations du service applicatif figurant dans le Certificat ne sont plus en conformité avec l'Identité cachet serveur ou l'utilisation prévue dans le Certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, CT, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

La révocation d'un Certificat devra être effectuée par le CT ou le Représentant Habilité (ou le cas échéant le MC en lieu et place du Représentant Habilité) :

- Soit sur demande faite auprès de l'AE pendant les heures ouvrées en remplissant une demande de révocation et en suivant les instructions données par l'AE par courrier électronique ou par téléphone ;
- Soit depuis le site web Portail d'AE à l'aide de son Code de révocation et de l'URL de révocation.

Seules les révocations effectuées sur l'interface web de l'AC sont prises en compte en 24H00.

Si le CT ou le Représentant Habilité (ou le Mandataire de Certification le cas échéant s'il en est désigné un) procède à une demande de révocation auprès de l'AE par tout autre moyen, la demande de révocation sera prise en compte dans les meilleurs délais durant les heures ouvrées de l'AE, suite à réception de la demande de révocation.

Il est précisé que l'AC et l'AE ne sont pas responsable de la perte par le CT, le Représentant Habilité ou le Mandataire de Certification du Code de révocation ou de la destruction, perte, ou non distribution du courrier électronique le contenant.

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

Le CT est informé qu'en cas d'expiration du contrat de Service conclu entre l'AE et l'AC quelle qu'en soit la cause, il pourra alors tout de même révoquer son Certificat via le site web de l'AC à l'aide de son Code de révocation. Il est du ressort de l'AE d'avertir le CT d'une telle rupture contractuelle.

8.2 Révocation à l'initiative de l'AC, l'AE

La révocation d'un Certificat sera immédiatement effectuée par l'AC, l'AE en cas de survenance d'une des circonstances suivantes :

- Les informations du service applicatif figurant dans le Certificat ne sont plus en conformité avec l'Identité cachet serveur ou l'utilisation prévue dans le Certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, CT, n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;

- La révocation de l'AC ;
- La fin de vie de l'AC ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Le CT concerné sera informé par courriel de la révocation de son Certificat dès que la révocation de son Certificat a été effectuée.

9 Prise d'effet et durée

Les présentes CGU prennent effet à compter de la date de leur signature par le CT et le Représentant Habilité ou le MC, concomitante à la date de demande de Certificats. Les Conditions Générales sont applicables pendant une durée similaire à la durée de vie des Certificats émis pour le CT et prennent fin à la date de fin de validité desdits Certificats.

Dans l'hypothèse où la Demande de Certificat est rejetée par l'AE, et que le CT n'a pas communiqué à l'AE le complément d'informations nécessaires à la recevabilité de son dossier sous un délai d'un (1) mois à compter de la notification du rejet, la Demande sera caduque.

10 Obligations du CT, du Représentant Habilité et du MC

10.1 Obligations du Représentant Habilité

Le Représentant Habilité de l'Entité Légale du CT s'engage à respecter les stipulations des présentes Conditions Générales et la Politique de Certification. A cet égard, il est responsable :

- De l'authenticité et la véracité des informations communiquées dans le dossier de Demande de Certificat ainsi que les documents qui accompagnent ces informations ;
- De la demande, sans délai, de la révocation d'un Certificat auprès de l'AE dès lors qu'elle est nécessaire, et notamment en cas de vol, divulgation, suspicion de compromission ou compromission de la clé privée d'un Certificat ou de changement de l'Identité Cachet serveur au sein de l'Entité légale ;
- De l'information sans délai, de toute modification relative aux informations des Certificats et/ou des documents du CT ou du MC, auprès de l'AE ;
- De se tenir informé, via le site Web de l'AE, de l'évolution des présentes Conditions Générales d'utilisation des Certificats ;
- De désigner, lorsque cela est nécessaire, les Mandataire de Certification et à ce titre signer les Formulaires de Création de Mandat ;
- De la protection en confidentialité et intégrité du Code de révocation et du courrier électronique contenant l'URL de révocation.

10.2 Obligations du Mandataire de Certification

Le Mandataire de Certification s'engage à respecter les stipulations des présentes Conditions Générales et la Politique de Certification.

A cet égard, le Mandataire de Certification est responsable :

- De l'authenticité et la véracité des informations communiquées dans le dossier de Demande de Certificat ainsi que les documents qui accompagnent ces informations ;
- De la demande, sans délai, de la révocation d'un Certificat auprès de l'AE dès lors qu'elle est nécessaire, et notamment en cas de vol, divulgation, suspicion de compromission ou compromission de la clé privée d'un Certificat ou de changement de l'Identité Cachet serveur au sein de l'Entité légale ;
- De l'information sans délai, de toute modification relative aux informations des certificats et/ou des documents du CT et du Représentant Habilité auprès de l'AE ;
- De se tenir informé, via le site Web de l'AE, de l'évolution des présentes Conditions Générales d'utilisation des Certificats ;
- De la signature du mandat de certification auprès de l'AE ;
- De la transmission des demandes de certificat(s) pour l'Entité Légale qu'il représente ;
- De la présentation des pièces justificatives des Utilisateurs requises pour l'obtention d'un certificat ;
- Le cas échéant, de la transmission du formulaire de refus de certificat à l'AE ;
- De la demande de révocation d'un Certificat auprès de l'AE dès lors qu'elle est nécessaire, et notamment en cas de vol, divulgation, suspicion de compromission ou compromission de la clé privée d'un Certificat ou de changement de situation du CT au sein de l'Entité légale ;
- De la protection en confidentialité et intégrité du Code de révocation et du courrier électronique contenant l'URL de révocation.
- De la réception et remise aux CT du Support avec authentification en face-à-face.

10.3 Obligations du CT

Le CT s'engage à respecter les stipulations des présentes Conditions Générales et la Politique de Certification. A cet égard, il est responsable :

- De l'exactitude et complétude des informations transmises dans le cadre d'une Demande de Certificat ;

- De la protection en confidentialité et en intégrité du Code d'activation, des Certificats et des Clés privées associées qui lui sont fournis ;
- Du changement du Code d'activation avant toute utilisation dans une application de sa clé privée suite à la réception de son support ;
- De Vérifier l'état de son certificat (Non expiré et non révoqué) avant toute utilisation ;
- Des équipements et des logiciels permettant d'utiliser les Certificats et la clé privée afin de respecter les exigences de la PC ;
- De l'utilisation des Certificats et des Clés privées associées conformément aux stipulations de l'article 5 ci-avant et de la Politique de Certification ;
- De l'authenticité et la véracité des informations communiquées dans le dossier de Demande de Certificat remis à l'AE ainsi que les documents qui accompagnent ces informations ;
- De la demande, sans délai, de la révocation d'un Certificat auprès de l'AE dès lors qu'elle est nécessaire, et notamment en cas de vol, divulgation, suspicion de compromission ou compromission de la clé privée d'un Certificat ou de changement de l'Identité Cachet serveur au sein de l'Entité légale. Le CT s'interdit d'utiliser un Certificat suite à l'expiration de celui-ci, à une demande de Révocation ou à la notification de la Révocation du Certificat, quelle qu'en soit la raison ;
- De l'information sans délai, de toute modification relative aux informations des certificats et/ou des documents auprès de l'AE ;
- De se tenir informé, via le site Web de l'AE, de l'évolution des présentes Conditions Générales d'utilisation des Certificats ;
- D'adresser sans délai à l'AE une demande de reproduction de Support en cas de non réception de celui-ci ;
- De la protection en confidentialité et intégrité du Code de révocation et du courrier électronique contenant l'URL de révocation.

D'une manière générale, le CT doit prendre toutes les mesures nécessaires pour assurer la sécurité et l'intégrité des données ainsi que celles des moyens informatiques sur lesquels il utilise le Code d'activation, les Certificats et les bi-clés. Il s'engage à prendre toutes les mesures propres à assurer la sécurité physique et logique de sa Clé privée et du Certificat. En outre, il est seul responsable de la protection de sa (ou ses) Clé(s) privée(s) conservée(s) dans le Support, contre la violation, la perte, la divulgation, la modification et l'usage abusif.

En outre, le Code d'activation étant personnalisable, il est fortement conseillé au CT de le modifier régulièrement et de le constituer d'au moins quatre (4) caractères alphanumériques (chiffres) afin de garantir la sécurité des clés étant précisé que l'AE et l'AC ne saurait être tenue responsable de la compromission du Code d'activation.

Au cas où les informations contenues dans le Certificat changeraient, le CT doit sans délai en informer l'AE par écrit, en établissant une demande de Révocation, qui permettra de révoquer le Certificat concerné. Le CT s'engage dans ce contexte à ne plus utiliser le Certificat concerné, quelle qu'en soit la raison.

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

12 Service Clients et Qualité de Service de l'AE

Un service clients est mis à disposition par l'AE et traitera les questions relatives à l'utilisation du Certificat. Le service clients est exclusivement actionné par le Représentant Habilité, le Mandataire de Certification ou le CT. Dès lors que le CT a contracté avec une AE, celle-ci devient la seule interface du CT pour toutes les questions relatives aux Certificats et le CT ne doit pas contacter l'AE directement. Les horaires d'ouverture du service clients de l'AE sont définies dans la zone réservée à l'AE dans le formulaire.

L'AC fournira soit à l'Opérateur central d'AE, soit au CT le cas échéant, une prestation de suivi des incidents de service, étant précisé que les incidents de service s'entendent uniquement sur les fonctionnalités de révocation en ligne des Certificats, ainsi que des fonctionnalités d'OCSP lors de la signature des documents.

En ce qui concerne les questions relatives au fonctionnement du Support et de ses logiciels associés, le service-clients de l'AC traitera ces dysfonctionnements conformément aux conditions générales du fabricant communiquées au CT lors de leur remise au CT.

En ce qui concerne la garantie relative au Support, l'AE assurera le remplacement de l'élément défectueux pendant toute la durée de vie du Certificat. Le retour du matériel défectueux pour remplacement auprès de l'AE est à la charge du CT.

13 Responsabilité

L'AC n'est pas responsable des préjudices indirects ou imprévisibles subis par le CT, le Représentant Habilité et le MC tels que préjudice financier ou commercial, perte de bénéfice, perte d'exploitation, perte de clientèle, trouble commercial, manque à gagner, perte de données trouvant leur origine ou étant la conséquence des présentes Conditions Générales ou inhérents à l'utilisation des Certificats émis par l'AC.

Dans le cas où la responsabilité de l'AC serait retenue, il est expressément convenu que l'AC sera tenue à la réparation des dommages directs certains et immédiats, dans une limite qui ne saurait excéder, tous sinistres confondus, la somme de trois millions de francs CFA (3 000 000 CFA). L'AC exclut toute responsabilité en cas de non-respect par le CT, le Représentant Habilité et le MC des engagements prévus aux présentes.

L'AC décline toute responsabilité à l'égard de l'usage des Certificats ou bi-clés associées émis par elle dans des conditions et à des fins autres que

celles prévues dans la Politique de Certification.

L'AC n'ayant aucune connaissance du contenu ou de la portée juridique du message ou document signé à l'aide des Certificats, sa responsabilité ne saurait être en aucun cas engagée sur ce fondement.

L'AC n'assume aucun engagement ni responsabilité quant à la qualité de la liaison Internet et aux conséquences dues à des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, ni quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication. Il est également convenu que l'AC ne peut être tenue responsable d'éventuels dysfonctionnements sur le poste du CT si ces dysfonctionnements font suite à l'utilisation du Certificat qui ne serait pas conforme à la documentation associée, ou aux instructions de l'AC ou le cas échéant aux formations dispensées par cette dernière. De même, la responsabilité de l'AC ne s'étend pas au bon fonctionnement (panne, erreur, incompatibilité, etc.) des matériels et logiciels du CT et de son environnement. L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant des présentes lorsque les circonstances y donnant lieu relèvent de la force majeure tel que défini à l'article 14 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 évènement 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 CT, des Représentants Habilités et des MC lors d'une Demande de Certificat font l'objet d'un traitement informatique par l'AC, de l'AE, aux seules fins de permettre (i) leur authentification et leur identification par l'AE et/ou le MC le cas échéant, (ii) la réalisation des vérifications nécessaires à la délivrance d'un Certificat et le cas échéant à sa révocation, et (iii) la construction de leur Identité Professionnelle 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 clients 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 Confidentialité

Le CT, le Représentant Habilité et le MC s'engagent à conserver confidentielles toutes les informations fournies par l'AC dans le cadre de l'exécution des présentes, 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 ou financière, toute information sur le savoir-faire, tous brevets, toutes marques, tous dessins, tous modèles, toutes définitions, toutes spécifications, tous comptes rendus de réunion, (ci-après désignées « Informations Confidentielles ») et à ne pas les divulguer à des tiers, pendant toute la durée des présentes conditions générales ainsi que pendant une période de cinq (5) années suivant l'expiration ou la résiliation de celles-ci.

En outre, la Clé privée associée au Certificat, les Codes d'activation, les Codes de révocation, les logiciels les composant, ainsi que toute documentation y afférentes constituent des Informations Confidentielles au sens du présent article.

Le terme "Information Confidentielle" signifie toute information donnée par l'AC au CT, sauf :

- Si le CT, le Représentant Habilité et/ou le MC les possédait avant la date de leur communication par l'AC ;
- Si elles étaient dans le domaine public avant la date de leur communication par l'AC, ou si elles y sont entrées par la suite sans qu'une faute puisse être imputée au CT, au Représentant Habilité et/ou au MC ;
- Si le CT, le Représentant Habilité et/ou le MC les a reçues d'un tiers, lui-même autorisé à les divulguer, sans mention faite au CT d'obligation de secret.
- Le CT, le Représentant Habilité et le MC recevant les Informations Confidentielles s'engagent à :
 - Ne pas divulguer et/ou communiquer ces informations à des tiers sous une forme quelconque sauf accord préalable écrit de l'AC ;
 - Ne communiquer les Informations Confidentielles qu'aux membres de son personnel ayant à en connaître, le CT se portant garant du respect par son personnel des présentes stipulations ;
 - Assurer de manière générale, leur sécurité en mettant en œuvre les mesures techniques et d'organisation appropriées pour les protéger contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés ;
 - Ne pas utiliser ces Informations Confidentielles, si ce n'est pour exécuter ses engagements dans le cadre des présentes ;
 - Mettre en œuvre les mesures nécessaires pour assurer le caractère confidentiel de ces informations ;
 - Ne pas déposer de demande de brevet, ou tout autre titre de propriété industrielle, ni invoquer tout droit de propriété intellectuelle incluant les Informations Confidentielles ;
 - Restituer à l'AC, ou détruire les documents confidentiels au terme des présentes, et ce quelles qu'en soient les causes d'extinction, ainsi que toute copie de ces documents qui en aurait été faite, sur quel que support que ce soit.

17 Propriété intellectuelle

17.1 Titularité des droits

Le CT, le Représentant Habilité et le MC reconnaissent que l'AC conserve tous les droits de propriété intellectuelle (brevet, marque déposée et autres droits) sur les éléments composant le Service, ainsi que la documentation, les concepts, techniques, inventions, procédés, logiciels ou travaux développés relativement aux Certificats et aux Services associés mis à disposition par l'AC, quels que soient la forme, le langage, le support des programmes ou la langue utilisée. Les présentes Conditions Générales ne confèrent au CT aucun droit de propriété intellectuelle relatif aux Certificats et aux Services associés.

Le CT, le Représentant Habilité et le MC s'interdisent tout agissement ou acte pouvant porter atteinte directement ou indirectement, ou par l'intermédiaire de tiers auxquels il serait associé, aux droits de propriété intellectuelle de l'AC sur les Certificats et les Services associés. En cas de tentative de saisie ou toute forme de contestation des droits de l'AC, le CT devra en aviser immédiatement l'AC et élever toute protestation contre la saisie, prendre toute mesure pour faire connaître les droits de propriété en cause.

Le CT, le Représentant Habilité et le MC s'engagent à prendre à l'égard de son personnel et/ou de tout tiers qui aurait légitimement accès aux services de certification, toutes les mesures nécessaires pour assurer le respect du droit de propriété sur les éléments logiciels composant le Service. Le CT, le Représentant Habilité et le MC s'engagent notamment à prendre toutes dispositions pour que son personnel ou les tiers susvisés ne conservent aucune documentation en-dehors de ses locaux.

17.2 Droits concédés

Au titre des présentes, l'AC concède au CT un droit de propriété sur le Support et Code d'activation associé (sauf pour les Certificats d'AC nécessaires à la validation du Certificat du CT qui sont la propriété de l'AC), ainsi qu'un droit non exclusif, personnel et incessible d'utilisation des Services associés au Certificat à compter de la date de prise d'effet des présentes, pour la durée de vie du Certificat et pour la Côte d'Ivoire entière, sous réserve du paiement effectif par le Client du prix de l'abonnement annuel convenu.

Le CT est informé que le droit d'utilisation des Services associés au Certificat est conditionné à l'engagement préalable de :

- Respecter les prérequis techniques nécessaires au bon fonctionnement des Services associés communiqués par l'AC,
- Faire évoluer sa configuration technique suivant les recommandations faites par l'AC en cas de mise à jour des Services associés.

L'AC concède également aux CT un droit d'utilisation personnel et non cessible sur le Portail d'AE (service révocation) pour les seules fins de révocation de Certificats.

Le CT, le Représentant Habilité et le Mandataire de Certification s'engagent à n'utiliser les Services associés et le Portail d'AE que conformément aux autorisations fournies par l'AC et conformément à leur destination. Il est notamment interdit au CT, au MC et au Représentant Habilité de procéder, directement ou indirectement, à titre onéreux ou gracieux, de manière volontaire ou par l'effet d'une négligence, à toutes les opérations suivantes :

- Représentation, télétransmission, diffusion, mise en réseau ou distribution de tout ou partie des Services associés quel qu'en soit le moyen ;

- Utilisation des Services associés aux fins de conception, réalisation, diffusion ou commercialisation d'un service ou d'un élément logiciel le composant, réalisé par l'AC et objet des présentes ;
- Adaptation, modification, transformation, décompilation, contournement du code, notamment son système de protection des licences, transcription ou traduction des éléments logiciels utilisés dans le cadre des Services associés ;
- Utilisation contraire à la documentation des Services associés ;
- Utilisation des Services associés aux fins de concurrencer directement ou indirectement l'AC ;
- Utilisation des Services associés déléguée à un tiers non autorisé par l'AC dans le cadre d'une externalisation des services du CT.

L'utilisation des Services associés par le CT, non conforme à sa destination et non expressément autorisée par l'AC, pourrait être illicite et faire l'objet d'une sanction, notamment au titre du délit de contrefaçon.

Elle causerait en outre à l'AC un préjudice certain devant faire l'objet d'une réparation. En aucun cas, la responsabilité de l'AC ne saurait être engagée en raison d'une utilisation des Services associés non conforme à sa destination et non expressément autorisée par l'AC, faite par le CT, le Représentant Habilité, le Mandataire de Certification, tous salariés, agents ou sous-traitant.

D'une manière générale, le CT s'interdit d'utiliser de modifier ou de transférer, de décompiler, de désassembler, de traduire les éléments logiciels composant les services associés, en dehors des conditions expressément précisées aux présentes Conditions Générales d'Utilisation.

Il est précisé que le Représentant Habilité de l'Entité légale du CT signant la Demande de Certificats est soumis aux obligations du présent article.

18 Sous-traitance

Les CT et le Représentant Habilité autorisent expressément l'AC à communiquer à ses éventuels sous-traitant les données nécessaires à l'exécution des prestations sous-traitées.

19 Divers

20.1 Cession des Conditions Générales

Le CT, le Représentant Habilité et le Mandataire de Certification s'interdisent de céder le Conditions Générales ainsi que les droits et obligations pris séparément sans l'accord exprès et préalable de l'AC.

20.2 Assurance

L'AC atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations relatives aux présentes.

20.3 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 des Conditions Générales d'Utilisation impossible ou déséquilibrée par rapport aux conventions initiales.

21.4 Notification

Toute notification adressée au titre des présentes sera envoyée par lettre recommandée avec avis de réception adressée au siège sociale des Parties. Toute réclamation du CT devra, sous peine de forclusion, être adressée par lettre recommandée avec accusé de réception à l'AE ou directement à l'AC dans un délai d'un (1) mois suivant la survenance de l'événement motivant ladite réclamation.

22 Attribution de juridiction - Loi applicable

En cas de litige sur l'interprétation, la validité ou l'exécution des présentes Conditions Générales, les Parties conviennent de chercher un règlement amiable ; Si les Parties ne parviennent 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 sur injonction de payer.