

DEMANDE CERTIFICAT PERSONNE PHYSIQUE

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

Raison sociale de l'AE		CRYPTONEO
	Informations de contact Service Clients	
	Téléphone	(+225) 27 22 50 17 25
	Adresse e-mail	serviceclient.tsp@cryptoneo.com
	Heures d'ouverture	8h30 - 12h 14h30 - 17h

Zone réservée à l'entité en charge de la remise

Adresse Postale de l'entité en charge de la remise	
Nom de l'entité en charge de la remise	CRYPTONEO
Nom de l'opérateur de remise (option)	CRYPTONEO
Rue	Cocody 2 plateaux 7ème tranche, Rue L 125
Code Postal	28 BP 657 Abidjan 28
Ville	Abidjan
Pays	Côte d'Ivoire
E-mail de notification	serviceclient.tsp@cryptoneo.com

Nota Bene : toutes les pages doivent être paraphées par tous les signataires.

Zone réservée au Représentant Habilité ou Personne Autorisée**AVERTISSEMENT**

Cette Page contient les informations relatives à l'Entreprise ou la Structure Administrative à laquelle le Porteur est rattaché.

Tous les champs doivent être vérifiés et remplis.

Nom de l'entreprise ou structure administrative tel que noté sur la DFE ou équivalent	
Numéro CC / Numéro Décret / IDU (CEPICI)	
Site Internet (Optionnel)	

☐ **Mandataire de Certification**☐ **Représentant habilité ou Personne Autorisée**

Référence du mandat (Si Mandataire de Certification)	
Nom	
Prénom(s)	
Téléphone Bureau	
E-mail	

Durée de Vie du Certificat

☐**1 an**☐**2 ans**☐**3 ans****NOM** (Représentant Habilité / MC)**Prénom(s)** (Représentant Habilité / MC)**Je, soussigné,**

--

--

vous prie d'enregistrer la demande de Certificat pour le PORTEUR identifié dans cette demande.

Je certifie que la copie de sa pièce d'identité officielle est conforme à l'original et que cette dernière est valide à la date de signature de cette demande.

Pièces Justificatives Entité Légale / Représentant Habilité / Mandataire de Certification

Page à remplacer par

- **Pour une Entreprise**
 - La copie de la DFE justifiant l'existence de ladite entreprise
 - Au besoin, la copie d'un document Administratif légal de l'Entreprise mentionnant le représentant habilité

- **Pour une administration ou une association**
 - La copie d'un document justifiant la délégation de l'autorité responsable de la Structure Administrative ou de l'Association qui fera office de Représentant Habilité ou de personne autorisée. (Décret, Arrêté de nomination ou Procès-verbal)

Zone réservée au PORTEUR

AVERTISSEMENT

Cette page contient les informations concernant le Porteur.

Tous les champs doivent être vérifiés et remplis.

Nom du porteur (tel que sur la Pièce d'identité)	
Prénom(s) du porteur (tel que sur la Pièce d'identité)	
Fonction du porteur	
E-mail du porteur	
Numéro de téléphone (Portable) (identifié suivant le Décret n°2017-193 du 22 mars 2017 portant identification des abonnés des services de télécommunications/TIC)	

Adresse postale pour la réception du courrier

Ville	
Localisation	
Boîte Postale	
Pays	CI

Type et numéro de pièce d'identité du PORTEUR.

- ☐ Carte d'identité biométrique ☐ Passeport biométrique ☐ Permis de conduire biométrique
- ☐ Carte consulaire biométrique ☐ Titre de séjour biométrique

Numéro de la pièce justificative d'identité du Porteur	
--	--

Intégrez une copie de la Pièce d'identité à la page suivante.

(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.)

Pièce Justificative du PORTEUR

Page à remplacer par

**La photocopie recto verso de la pièce d'identité du
PORTEUR.**

Condition d'usage du Certificat

Les signataires ont pris connaissance et acceptent les termes et conditions d'usage des Certificats tels que décrits dans les Politiques de Certification (OID 1.3.6.1.4.1.46116.1.4.101.11) accessibles à l'adresse suivante <https://www.cryptoneo.com> et dans les Conditions Générales d'Utilisation (CGU) jointes au présent formulaire, notamment les usages ci-dessous. L'Autorité de Certification émettrice des Certificats est dénommée « **AC CRYPTONEO PERSONNES** ».

En acceptant les Conditions Générales (CGU), le PORTEUR reconnaît avoir pris connaissance et être lié par les termes de la Politique de Certification.

Gestion des données à caractère personnel

Les signataires acceptent que les données personnelles les concernant recueillies lors de la demande de certificats fassent l'objet d'un traitement informatique aux fins :

- D'être authentifiés par l'AE et/ou le Mandataire de Certification ;
- De permettre les vérifications nécessaires à la délivrance des certificats, à leur renouvellement et à leur révocation ;
- De permettre la construction de l'identité portée dans les certificats ;
- D'apporter les preuves nécessaires à la gestion des certificats des Porteurs.

Ces données peuvent également être traitées et transmises à des prestataires et partenaires pour les besoins de la fourniture du Service de Certification Électronique.

Il est ainsi précisé qu'en signant le présent formulaire de demande de certificat, les signataires acceptent expressément que leurs données à caractère personnel soient conservées par CRYPTONEO aux seules fins de traitement définies ci-avant et ce pendant une période de 10 ans à compter de l'acceptation expresse par l'AE de la demande de Certificats.

Les signataires sont informés de leurs droits de faire rectifier les informations personnelles les concernant dans la seule période de rétraction possible et prévue à cet effet, soit 15 jours après la publication du Certificat.

Toute modification de leurs données à caractère personnel doit être adressée au service client de CRYPTONEO dont les coordonnées sont fournies en début de formulaire.

Les signataires sont en outre informés que le fait de s'opposer à la conservation de leurs données personnelles empêche l'obtention du certificat concerné et rend ainsi caduque la demande de certificat correspondante.

Information de contact Correspondant à la protection des données à caractère personnel

Adresse électronique	cesar.nyamien@cryptoneo.com
Adresse postale	28 BP 657 Abidjan 28
Téléphone	+225 07 89 84 61 17

Porteur

J'atteste sur l'honneur de l'exactitude et de la véracité de l'ensemble des éléments d'information que j'ai fourni dans le cadre du présent formulaire ainsi que les pièces justificatives qui l'accompagne. Je déclare avoir pris connaissance des CGU ainsi que des modalités de traitement des données personnelles et les accepte sans réserve. J'accepte en outre d'utiliser la Signature Électronique pour valider mon engagement.

Date et Signature du Porteur

--	--

Mandataire, Représentant Habilité ou personne autorisée

J'atteste sur l'honneur de l'exactitude et de la véracité de l'ensemble des éléments d'information que j'ai fourni dans le cadre du présent formulaire ainsi que les pièces justificatives qui l'accompagne. Je déclare avoir pris connaissance des CGU ainsi que des modalités de traitement des données personnelles et les accepte sans réserve. J'accepte en outre d'utiliser la Signature Électronique pour valider mon engagement.

Date et Signature du Mandataire, du Représentant Habilité ou de la personne autorisée

--	--

Opérateur d'AE (Autorité d'Enregistrement)

J'atteste sur l'honneur avoir vérifié la complétude et la cohérence de ce dossier. J'accepte d'utiliser la Signature Électronique pour valider mon engagement. Je déclare avoir pris connaissance des modalités de traitement des données personnelles et les accepte sans réserve.

Nom, Prénom, Date et Signature de l'Opérateur d'AE

--	--

Nota Bene : toutes les pages doivent être paraphées par tous les signataires.

Conditions Générales 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 électronique et d'authentification délivrés par l'AC CRYPTONEO, ainsi que les obligations respectives du PORTEUR, du Représentant Habilité de l'Entité Légale à laquelle est rattaché le PORTEUR 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. CRYPTONEO est AC. L'AC utilisée est l'AC « **AC CRYPTONEO 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 PORTEUR, l'Entité Légale à laquelle est rattaché le PORTEUR, ou le cas échéant le Mandataire de certification désigné par l'Entité Légale, (ii) enregistrer les demandes d'émission, de renouvellement et de révocation de Certificats, et les valider ou les rejeter, (iii) après validation d'une demande de Certificat, générer des bi-clés sur supports cryptographiques et générer les codes PIN associés auxdits Certificats, (iv) adresser les Codes PIN aux PORTEURS. CRYPTONEO 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 numérique et la Clé publique associée à la clé privée contenue dans le Support Cryptographique. Le Certificat est signé électroniquement par l'AC « **AC CRYPTONEO PERSONNES** ».

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 PORTEURS 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 des valeurs de données qui sont nécessaires pour mettre en œuvre la Bi-clé à l'aide d'un logiciel informatique de Signature électronique. Le Code d'activation (ou code PIN) est adressé par l'AE au PORTEUR par courrier électronique ou par SMS.

Code de révocation : désigne le code défini et adressé par l'AE au PORTEUR, 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 PORTEUR et au Représentant Habilité (ou MC) de révoquer seul son Certificat via l'URL de révocation ou via 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 toute demande d'émission ou de renouvellement de Certificats effectuée par le PORTEUR sur le Formulaire prévu à cet effet. Chaque Demande est signée par le PORTEUR ainsi que, le cas échéant, le Représentant Habilité de l'Entité Légale auquel est rattaché le PORTEUR ou le Mandataire de certification désigné par l'Entité Légale.

Entité Légale : désigne la personne morale indiquée dans la Demande de Certificat, à laquelle le PORTEUR est rattaché, et fournisseur des services pour lesquels ce dernier utilise le Certificat Électronique.

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 de l'Entité Légale et celles définies par l'AC. Cette identité est utilisée pour authentifier un service applicatif d'une Entité Légale et/ou certifier des données numériques produites par une Entité Légale.

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

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Mandataire de Certification (MC) : désigne une personne physique mandatée par l'Entité Légale pour procéder, au nom et pour le compte de ce dernier, aux demandes de certificats auprès de l'AE. Le recours à un mandataire de certification (MC) n'est pas obligatoire.

Opérateur d'AE : désigne toute personne physique nommée expressément par l'AE pour la remise des certificats aux PORTEURS, ou le cas échéant au(x) MC, suivant les Procédures de gestion de Certificats de l'AC.

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

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'elle délivre. Ce document décrit également les obligations et responsabilités de l'AC, de l'AE, des PORTEURS 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 PORTEUR devra respecter les règles décrites dans la Politique de Certification (PC) applicable au Service, dont l'OID est 1.3.6.1.4.1.46116.1.4.101.11, et consultable à l'adresse web suivante : <https://cryptoneo.com>.

PORTEUR : Désigne la personne physique propriétaire d'un Certificat. Le PORTEUR 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 PORTEUR sont effectuées par l'AE. Le PORTEUR 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.

Procédures de gestion des Certificats : désigne l'ensemble des procédures édictées par l'AE que doivent respecter les Opérateurs d'AE, les PORTEURS, 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 PORTEUR 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 PORTEUR.

Représentant Habilité : désigne toute personne physique disposant des pouvoirs de représenter de par la loi, l'Entité Légale à laquelle est rattaché le PORTEUR. 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 PORTEURS. Dans la PC, le Représentant Habilité est appelé « Représentant Légal ».

Révocation (d'un Certificat) : désigne l'opération demandée par le PORTEUR, l'AC ou 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, pour permettre l'utilisation de Certificats et de bi-clé protégés par un code d'activation, incluant la mise à disposition d'un Portail d'AE pour la révocation en ligne.

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://www.cryptoneo.com>. Cette contremarque de temps a pour objet de positionner dans le temps la réalisation et l'acceptation de transaction conclue en ligne par l'intermédiaire de services applicatifs.

Service d'OCSP (Online Certificate Status 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 matériels et logiciels utilisés pour mettre en œuvre une 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 PORTEUR 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.

ARTCI : l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en charge de la délivrance des agréments aux Autorités de Certification en République de Côte d'Ivoire.

3 Procédure de demande de Certificat

Le PORTEUR 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 PORTEUR ainsi que par le Représentant Habilité de l'Entité Légale auquel est rattaché le PORTEUR 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 PORTEUR. 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 PORTEUR 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 PORTEUR et du Représentant Habilité ou le cas échéant du MC s'il en est désigné un (nom, prénom(s), numéro de téléphone et courrier électronique) sont transmis à l'AE.

4 Délivrance du Certificat, du Code de Révocation et du Code d'Activation

Après la génération du certificat, l'AE adresse au porteur :

- 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 PORTEUR indiquée sur le Formulaire de Demande de certificat ;
- Le Code de révocation au PORTEUR à l'adresse de courrier électronique indiquée sur le Formulaire de demande de certificat.

Toutefois, le PORTEUR, 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.

5 Modalités d'utilisation du Certificat

Le PORTEUR 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 PORTEUR pourrait être engagée. Il appartient au PORTEUR de s'assurer que les matériels dont il dispose, notamment son terminal, ses logiciels d'interrogations (navigateurs) ou ses moyens de connexions puissent 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 électronique de document ou message électronique et de contrôle d'accès en SSL/TLS auprès de serveur.

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. À 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 PORTEUR pourra renouveler le Certificat en effectuant une nouvelle Demande de Certificat auprès de l'AE conformément à la procédure qui lui sera indiquée par l'AE. Un nouveau Kit Certificat est distribué au PORTEUR. 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 PORTEUR

L'AE devra être avertie sans délai de toute demande de révocation de Certificat à l'initiative du PORTEUR 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 de l'Entité Légale et/ou du PORTEUR figurant dans le Certificat ne sont plus en conformité avec l'Identité du PORTEUR, ceci avant l'expiration normale du certificat ;
- Le demandeur, PORTEUR, 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 l'Entité Légale ;
- 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 PORTEUR 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 24h.

Si le PORTEUR 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 la réception de la demande de révocation transmise à l'AE.

Il est précisé que l'AC et l'AE ne sont pas responsables de la perte par le PORTEUR, le Représentant Habilité ou le Mandataire de Certification du Code de révocation ou de la destruction, perte 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.

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

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

- Les informations de l'Entité Légale et/ou du PORTEUR figurant dans le Certificat ne sont plus en conformité avec l'Identité du PORTEUR, ceci avant l'expiration normale du certificat ;
- Le demandeur, PORTEUR, 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 de l'Entité Légale ;
- 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 PORTEUR concerné sera informé par courriel ou par SMS 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 PORTEUR 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 PORTEUR 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 PORTEUR 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 PORTEUR, du Représentant Habilité et du MC

10.1 Obligations du Représentant Habilité

Le Représentant Habilité de l'Entité Légale s'engage à respecter les stipulations des présentes Conditions Générales et la Politique de Certification. À 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 l'information sans délai, de toute modification relative aux informations des Certificats et/ou des documents du PORTEUR 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 Mandataires 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. À 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 l'information sans délai, de toute modification relative aux informations des Certificats et/ou des documents du PORTEUR 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 PORTEURS requises pour l'obtention d'un Certificat ;
- De la demande de révocation d'un Certificat auprès de l'AE dès lors qu'elle est nécessaire, et notamment en cas de suspicion de compromission ou compromission de la clé privée d'un Certificat ;
- De la protection en confidentialité et intégrité du Code de révocation et du courrier électronique contenant l'URL de révocation.

10.3 Obligations du PORTEUR

Le PORTEUR s'engage à respecter les stipulations des présentes Conditions Générales et la Politique de Certification. À 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 ;
- 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. Le PORTEUR 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 ;
- De la protection en confidentialité et intégrité du Code de révocation et du courrier électronique ou du SMS contenant l'URL de révocation.

D'une manière générale, le PORTEUR 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 logique de sa Clé privée et du Certificat. En outre, il est responsable de la protection de sa (ou ses) Clé(s) privée(s) contre la violation, la perte, la divulgation, la modification et l'usage abusif.

Le PORTEUR s'engage à alerter l'AE dans les meilleurs délais en cas de perte de son terminal mobile ou en cas de changement de son numéro de téléphone ou de changement de détenteur de sa carte SIM ou de son adresse de courrier électronique indiqués dans le présent formulaire.

Au cas où les informations contenues dans le Certificat changeraient, le PORTEUR doit sans délai en informer l'AE, en établissant une demande de Révocation, qui permettra de révoquer le Certificat concerné. Le PORTEUR 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 PORTEUR. Les horaires d'ouverture du service clients de l'AE sont définis dans la zone réservée à l'AE dans le formulaire.

L'AE fournira au PORTEUR 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 cryptographique et de ses logiciels associés, le service-clients de l'AC traitera ces dysfonctionnements conformément aux conditions générales du fabricant et des éditeurs.

13 Responsabilité

L'AC n'est pas responsable des préjudices indirects ou imprévisibles subis par le PORTEUR, 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.

L'AC exclut toute responsabilité en cas de non-respect par le PORTEUR, 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 terminal du PORTEUR si ces dysfonctionnements font suite à l'utilisation du Certificat qui ne serait pas conforme à l'usage, 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 mauvais fonctionnement (panne, erreur, incompatibilité, etc.) des matériels et logiciels du PORTEUR 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

L'Entité Légale à laquelle est rattaché le porteur est informée 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 recherchée 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 PORTEURS, des Représentants Habilités et des MC lors d'une Demande de Certificat font l'objet d'un traitement informatique par l'AC, par 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 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 scan du Formulaire de demande de certificat au PORTEUR.

Les destinataires des données personnelles sont les personnels Techniques de l'AE et de l'AC, le correspondant à la protection des données à caractère personnel pour l'AE. Les données personnelles sont conservées 10 ans après l'expiration du Certificat.

16 Confidentialité

Le PORTEUR, 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 PORTEUR, sauf :

- Si le PORTEUR, 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 PORTEUR, au Représentant Habilité et/ou au MC ;
- Si le PORTEUR, le Représentant Habilité et/ou le MC les a reçues d'un tiers, lui-même autorisé à les divulguer, sans mention faite au PORTEUR d'obligation de secret.

Le PORTEUR, 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, l'Entité Légale se portant garante 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 autorisé ;
- 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 PORTEUR, 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 utilisés. Les présentes Conditions Générales ne confèrent au PORTEUR aucun droit de propriété intellectuelle relatif aux Certificats et aux Services associés.

Le PORTEUR, 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 PORTEUR 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 PORTEUR, 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.

17.2 Droits concédés

Au titre des présentes, l'AC concède au PORTEUR 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 du prix convenu pour les services fournis par l'AC et l'AE.

Le PORTEUR 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 PORTEURS un droit d'utilisation personnel et non cessible sur le Portail d'AE (service révocation) pour les seules fins de révocation de Certificats.

Le PORTEUR, 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 PORTEUR, 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 de l'Entité Légale.

L'utilisation des Services associés par le PORTEUR, 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.

D'une manière générale, le PORTEUR 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 l'Entité Légale signant la Demande de Certificats via son Représentant Habilité ou le MC, est soumis aux obligations du présent article.

18 Sous-traitance

Le PORTEUR et l'Entité Légale autorisent expressément l'AC à communiquer à ses éventuels sous-traitants les données nécessaires à l'exécution des prestations sous-traitées.

19 Cession des Conditions Générales

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

20 Assurance

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

21 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.

22 Notification

Toute notification adressée au titre des présentes sera envoyée par lettre recommandée avec avis de réception adressée au domicile des Parties. Toute réclamation du PORTEUR 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.

23 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.