Contrat d'abonnement au service de certification C@rteurope

Autorité de Certification : **CertEurope eID Website**

Pour le service confiance : **Authentification de site web**

Politique de Certification (OID) :

1.2.250.1.105.25.411.2.1.1.1.0, 1.2.250.1.105.25.411.2.1.2.1.0, 1.2.250.1.105.25.411.2.2.1.1.0
1.2.250.1.105.25.411.2.2.2.1.0
1.2.250.1.105.25.411.2.3.1.1.0, 1.2.250.1.105.25.411.2.3.2.1.0
1.2.250.1.105.25.411.1.4.1.1.0, 1.2.250.1.105.25.411.1.4.2.1.0
1.2.250.1.105.25.411.2.5.1.1.0, 1.2.250.1.105.25.411.2.5.2.1.0

Conditions Générales

Entre

CertEurope SAS, 26, rue du Faubourg Poissonnière, 75010 Paris, inscrit au registre du commerce de Paris sous le n° 434 202 180, représenté par son président Monsieur Stanislas de Rémur,
(Désignée ci-après par **CERTEUROPE**)

Et

L'ABONNE, personne physique ou morale qui désire utiliser un certificat électronique pour s'identifier sur des applications informatiques, signer des documents électroniques ou émettre des messages électroniques signés et dont l'identité portée dans les conditions particulières est contrôlée par une personne représentant l'Autorité d'Enregistrement habilitée par l'Autorité de Certification, (personne désignée par le terme AE), identifié dans les mêmes Conditions Particulières.

Il a été convenu ce qui suit.

1 Objet

Les présentes Conditions Générales définissent les conditions et modalités par lesquelles CERTEUROPE, agissant en qualité d'Autorité de Certification, met à la disposition de l'ABONNE le Service de Certification C@RTEUROPE (désigné ci-après par le « SERVICE »).

2 Définitions

Il est donné à chaque mot ci-après la signification suivante :

Abonné : personne physique agissant pour le compte d'une personne morale qui souscrit au Service de Certification Électronique C@rteurope.

ACPR : Autorité de contrôle prudentiel et de résolution est l'organe de supervision français de la banque et de l'assurance.

Autorité de Certification (également appelée Prestataire de Services de Certification) : personne morale qui délivre des certificats électroniques. Cette entité est responsable de la bonne gestion des certificats.

Autorité d'Enregistrement (**AE**): Fonction remplie par une personne désignée par l'Autorité de Certification C@rteurope qui consiste à vérifier l'identité et la qualité d'un demandeur de certificat et/ou à générer ledit certificat et/ou à révoquer ledit certificat. Au sein de la fonction d'Autorité d'Enregistrement, les rôles peuvent être subdivisés en :

- Autorité d'Enregistrement Administrative (**AEA**) : fonction qui consiste à vérifier l'identité et la qualité d'un demandeur de certificat avant de pouvoir procéder à la remise du certificat.
- Autorité d'Enregistrement Technique (**AET**) : fonction qui consiste à générer le certificat d'authentification serveur suite à une vérification préalable.
- Autorité d'Enregistrement Déléguée (**AED**) : fonction qui consiste à procéder à l'envoi du certificat au RCAS.

Bi-clé : une paire de bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptographie basée sur des algorithmes asymétriques.

Certificat électronique : Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme).

Certification : activité qui consiste à prendre la responsabilité d'émettre des certificats électroniques et à effectuer certains traitements techniques connexes. La certification est effectuée par une Autorité de Certification (ou **PSC**) ou encore par un Opérateur de Services de Certification (**OSC**) en sous-traitance de l'AC.

Déclaration des pratiques de certification (DPC) : énoncé des procédures organisationnelles et pratiques techniques effectivement respectées par une Autorité de Certification pour la gestion des certificats.

Directive sur les services de paiement (DSP2) : Directive européenne (UE) 2015/2366 adoptée le 25 novembre 2015. Elle décrit des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

European Banking Authority (EBA) : L'Autorité bancaire européenne a été créée par le règlement n° 1093/2010 du 24 novembre 2010 afin de renforcer le Système européen de supervision financière. Elle existe officiellement depuis le 1er janvier 2011 et succède au Comité européen des superviseurs bancaires.

EIDAS : Réglementation européenne **e**lectronic **ID**entification, **A**uthentication and trust **S**ervices.

Fully qualified domain name (FQDN) : nom de domaine qui indique la position absolue d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine (ex : www.certeurope.fr).

Infrastructure à Clé Publique (ICP) : ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

Liste de Certificats Révoqués (LCR) : liste de certificats ayant fait l'objet d'une révocation.

Mandataire de Certification : personne désignée par le représentant légal de l'entreprise pour effectuer les demandes de certificats et leur révocation pour les membres de l'organisme.

National Competent Authority (**NCA**) : autorité compétente nationale qui valide les rôles des prestataires de paiement. Une liste est disponible sur le site de l'EBA : https://eba.europa.eu/supervisory-convergence/supervisory-disclosure/competent-authorities

Dispositif de protection des clés privées : Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée.

Opérateur de Services de Certification (OSC) : composante de l'ICP disposant d'une plate-forme technique lui permettant de générer et émettre des certificats pour le compte d'une Autorité de Certification.

Politique de Certification (PC) : ensemble de règles édictées par une Autorité de Certification, qui définit les règles de gestion des certificats et le type d'applications auxquelles un certificat est adapté ou dédié. La PC est disponible sur https://www.certeurope.fr/chaine-de-confiance.

Prestataire de Service de Certification électronique (PSC) (également appelé "Autorité de Certification") : personne morale qui délivre des certificats électroniques. Dans le SERVICE présent, la prestation de certification électronique est fournie par CertEurope, qui joue le rôle de PSC.

Révocation d'un certificat : opération demandée par l'ABONNÉ, le RCAS, le Mandataire de Certification, l'AE ou l'AC au PSC et dont le résultat est la suppression, avant l'expiration de sa période de validité, de la garantie du PSC sur un certificat donné.

RCAS : personne physique responsable du Certificat d'Authentification Serveur, notamment l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'ABONNE.

Télé-procédures : procédures électroniques sécurisées permettant aux entreprises de transmettre aux services de l'Etat des déclarations administratives via Internet.

Vérificateur de la signature électronique : destinataire d'un fichier électronique signé qui procède au contrôle technique de la signature électronique.

3 Fournitures et prestations

Le SERVICE fourni est composé de prestations pris en charge par différentes entreprises sous-traitantes ou co-traitantes sous l'autorité et la coordination de CertEurope. Ces matériels et prestations comprennent :

- Une prestation de certification électronique, consistant en l'émission d'un certificat électronique de type : **Authentification de site web**

4 Dossier de souscription

CERTEUROPE a confié le soin de vérifier l'identité de la personne qui demande un certificat, de ses titres et qualités, à un intermédiaire de proximité nommé Autorité d'Enregistrement (AE). Cet intermédiaire ne saurait avoir de responsabilité par devant l'ABONNE.

L'Abonnement au SERVICE est souscrit par l'ABONNE avec CERTEUROPE par l'intermédiaire de L'AE. L'organisme identifié aux Conditions Particulières qui désire s'abonner doit fournir à L'AE les pièces suivantes dont le modèle est généralement fourni par L'AE :

- Le **"contrat d'abonnement au service de certification C@rteurope"** signé par le représentant légal ou le mandataire de certification ET le RCAS.
- **Un justificatif d'identité** du RCAS et du représentant légal sous forme de copies de documents en cours de validité (exemples : photocopies de la carte d'identité, du passeport, de la carte de séjour). Ces justificatifs doivent être certifiés conformes par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité).
- Le cas échéant **une lettre de procuration du représentant légal** de l'organisation désignant un Mandataire de Certification et une photocopie de sa pièce d'identité
- Le **KBIS original** de la société (datant de moins de trois mois) ou le **justificatif de l'activité professionnelle + Avis SIRENE** si le justificatif de l'activité professionnelle ne mentionne pas le numéro SIRENE.
- Le **numéro d'attestation du NCA** et **les rôles du prestataire de paiement** tels qu'ils figurent sur le registre du NCA.

5 Contrôles effectués au cours de la procédure d'abonnement

Lors de la saisie d'une demande d'abonnement, L'AE effectue les opérations de contrôle suivantes :

- Il vérifie l'identité du demandeur (RCAS et Mandataire de Certification ou RL), en s'assurant que la copie de sa pièce d'identité comporte sa photo et sa signature.
- Il vérifie l'existence de l'organisation en vérifiant son extrait **K-bis** ou **le justificatif de l'activité professionnelle et avis SIRENE.**
- Il vérifie éventuellement le Mandat du représentant légal au RCAS ou au Mandataire de certification si le RCAS n'est pas le représentant légal.
- Il vérifie chaque FQDN selon les modalités prévues par la réglementation EIDAS et les exigences du CA/B Forum.
- Vérifier le numéro d'attestation et les rôles du prestataire sur le registre de l'autorité national compétente.
  - Pour la France, le REGAFI : https://www.regafi.fr/spip.php?rubrique1
  - Pour d'autres pays européen, le registre EBA: https://euclid.eba.europa.eu/register/

L'AE doit authentifier le RCAS lors d'un face-à-face physique en vérifiant sa pièce d'identité originale.

6 Génération et durée de vie de la bi-clé

La bi-clé du certificat d'authentification de site web est générée par l'ABONNE selon les exigences de la norme ETSI TS 119 312.

La bi-clé doit être au format RSA, d'une longueur de 2048 bits et avec l'algorithme de calcul d'empreinte SHA-256.

La durée de vie de la bi-clé varie entre **12** et **24** mois.

7 Utilisation des certificats

CERTEUROPE garantit par les présentes que les certificats qu'il émet peuvent être utilisés dans les cas suivants :

- Etablissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager,
- Etablissement d'une session sécurisée entre un serveur et un agent,
- Etablissement d'une session sécurisée entre deux serveurs.

Les composants techniques du service de certification C@RTEUROPE sont conformes aux exigences fixées par la législation française ainsi qu'à la réglementation européenne n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».

8 Obtention du certificat

La création du certificat d'authentification serveur est faite par les Autorités d'Enregistrement effectuant une demande via l'infrastructure technique mise à leur disposition par CertEurope. L'AE se chargera de réunir et de vérifier les informations nécessaires à l'obtention du certificat par son client ABONNE.

La date et l'heure de l'émission d'un certificat sont déterminées avec précision grâce à une datation sécurisée mise en place par CERTEUROPE. Le certificat est valable de **12** à **24** mois suivant son émission dans la limite de validité de la bi-clé.

Les certificats, les LCR et les logs ainsi que les journaux d'évènements du cycle de vie du certificat sont archivés par CertEurope pendant sept (7) ans à partir de leur date d'expiration.

9 Révocation du certificat

9.1 Modalités

LE RCAS, LE MANDATAIRE DE CERTIFICATION ou LE REPRESENTANT LEGAL DE L'ENTREPRISE peut saisir à tout moment CERTEUROPE d'une demande de révocation.

Les demandes de révocations peuvent être transmises :

- Par courrier ou télécopie signé
- En se présentant au bureau de l'AE muni d'une pièce d'identité originale

9.2 Causes de révocation

La révocation du certificat doit être demandée dans les cas suivants :

- Tout événement affectant les pouvoirs du RCAS ;
- Les informations figurant dans le certificat ne sont plus en cohérence avec l'utilisation prévue du certificat et ce, avant l'expiration normale du certificat ; Par exemple si le rôle du prestataire de paiement a été révoqué par le NCA
- Le RCAS n'a pas respecté les modalités applicables d'utilisation du certificat ;
- La clé privée associée au certificat est suspectée de compromission, est compromise, est perdue ou volée ;
- Le certificat de l'Autorité de Certification C@rteurope doit être révoqué ;
- La cessation d'activité de l'ABONNE ou la cessation d'activité de l'AC CERTEUROPE.

Un certificat peut être révoqué à l'initiative de l'AE ou de l'AC dans les cas suivants :

- Non renouvellement du contrat par l'ABONNE à la date anniversaire de la génération à la demande de CERTEUROPE ou de L'AE pour défaut de paiement ;
- Décision de changement de composante de l'AC ou de l'AE suite à non-conformité des procédures de la DPC ;
- Cessation d'activité de l'organisme du RCAS

Le certificat dont la révocation a été demandée à CERTEUROPE est placé sans délai dans la liste des certificats révoqués. En cas d'utilisation de la procédure de révocation d'urgence, le temps de traitement, incluant la publication ne devra pas dépasser 72h.

La LCR, les PC, les DPC et les CGUs sont publiés et accessibles au public sur des serveurs disponibles 24 heures sur 24 et 7 jours sur 7.

9.3 Fin de vie de l'AC

Après terminaison d'une de ses AC, CertEurope, en accord avec les exigences de la norme ETSI EN 319 411-1/2, publiera une dernière CRL en assignant la valeur "99991231235959Z" au champ "nextUpdate", sauf exigences complémentaires de l'organe de supervision national (ANSSI).

Les informations sur le statut de révocation (CRL et OCSP) seront disponibles au moins 5 ans après la terminaison de l'AC.

La fin de vie fait l'objet d'une information clairement diffusée au moins sur le site de CertEurope et éventuellement relayée par d'autres moyens (associations, clubs utilisateur, réseaux sociaux, etc.).

En plus des éventuelles recommandations de l'ANSSI, CertEurope doit informer tous les Porteurs, Mandataires de Certification et les autres entités en lien avec l'AC (plateforme de marché, fournisseurs d'identités, etc.).

10 Obligations de l'abonné

En contrepartie du SERVICE fourni, l'ABONNE devra acquitter une facturation dont le coût et les modalités de paiement sont communiqués par l'AE.

De plus, l'ABONNE a les obligations suivantes :

- Communiquer des informations exactes lors de son enregistrement auprès de l'AE qui procédera à la demande de certificat auprès de CERTEUROPE, ainsi que toute modification de celles-ci ;
- Informer l'AE, dans les 16 jours après réception de son certificat, d'une éventuelle erreur. Passé ce délai, le certificat sera considéré comme accepté par le RCAS.
- Assurer l'hébergement du certificat
- Assurer la sécurité du serveur sur lequel est intégré le certificat.
- Respecter les conditions d'utilisation de la clé privée et du certificat correspondant ;
- Demander à CertEurope la révocation de son certificat dès l'occurrence d'une des causes définies au 9.2.

La responsabilité de l'Autorité d'Enregistrement ou de l'Autorité de Certification ne sera pas engagée si l'ABONNE, ou le représentant légal de la société, ou le mandataire de certification, a négligé ou tardé de les informer de tout événement ou modification susceptible de modifier les pouvoirs du RCAS.

11 Obligations du RCAS

La bi-clé est sous la responsabilité du RCAS. Lors d'actions effectuées sur le serveur comportant le certificat d'authentification serveur, le RCAS s'engage à respecter les exigences EIDAS et notamment la norme ETSI TS 119 312 pour :

- La génération la clé privée
- La méthode de transfert de la clé privée
- La mise en œuvre un processus de désactivation de la clé privée
- La mise en œuvre un processus de destruction de la clé privée

12 Données personnelles et confidentielles

Les données à caractère personnel recueillies sont indispensables pour l'exécution du contrat, dans le respect des règlementations applicables, notamment du règlement (UE) 2016/679 du 27 avril 2016. Le responsable du traitement est CertEurope en sa qualité d'Autorité de Certification.

Le traitement a pour finalité de permettre la gestion du cycle de vie des certificats (notamment la délivrance, le suivi, la révocation et le renouvellement), le support technique l'accompagnant, et le cas échéant, la facturation et le recouvrement. Les données à caractère personnel collectées par l'Autorité de Certification via son Autorité d'Enregistrement sont conservées pendant sept (7) ans à compter de la date d'expiration du dernier Certificat électronique délivré au Porteur, conformément à la Politique de Certification. Les données à caractère personnel collectées sont traitées et hébergées en France et en Union Européenne. Les données à caractère personnel traitées sont destinées aux services internes de l'Autorité de Certification et de l'Autorité d'Enregistrement, à leurs partenaires, sous-traitants ainsi qu'aux établissements bancaires.

Les personnes concernées disposent d'un droit d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition et de portabilité, dans les conditions prévues par le règlement (UE) 2016/679 du 27 avril 2016, ainsi que du droit de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès, qu'elles peuvent exercer en contactant CertEurope par courrier postal à l'adresse « CertEurope, DPO, 26 rue du Faubourg Poissonnière, 75010 Paris » ou sur privacy@oodrive.com. Les personnes concernées sont averties que le bénéfice de ces droits pourrait être limité, notamment pour répondre à des contraintes règlementaires. La copie d'une pièce d'identité en cours de validité pourra être demandée par CertEurope afin de vérifier l'identité du demandeur.

Les personnes concernées disposent de la faculté d'introduire une réclamation auprès du Délégué à la Protection des Données ou DPO de CertEurope sur privacy@oodrive.com ou, le cas échéant, auprès de l'autorité de contrôle (CNIL, 3 Place de Fontenoy, 75007 Paris).

Le dossier d'enregistrement de l'Abonné et notamment les données personnelles sont considérées comme confidentielles par CertEurope qui en assure l'archivage.

L'AE et CertEurope n'ont à aucun moment connaissance de la clé privée du Porteur qui reste sous la responsabilité exclusive de celui-ci.

13 Information de l'abonné

L'AE ou CERTEUROPE informe l'ABONNE de tout événement significatif concernant la communauté des ABONNES, notamment en cas de compromission de la clé privée de CERTEUROPE ou en cas de révocation de leur certificat.

14 Responsabilité et assurances

CERTEUROPE doit fournir des prestations de certification électronique conformes à l'état de l'art et aux prescriptions des textes légaux et réglementaires. Il doit fournir un service de qualité permanent, et continu pour toute la durée de validité du certificat de l'ABONNE, correspondant aux diverses obligations énumérées par les présentes. A défaut, il s'expose à la résiliation unilatérale du contrat par l'ABONNE et à la mise en jeu de sa responsabilité.

Cependant, CERTEUROPE ne peut en aucun cas être tenue responsable de tout dommage indirect au sens de la jurisprudence des juridictions françaises.

La responsabilité éventuelle de CERTEUROPE en raison de l'exécution de ses obligations contractuelles est limitée au montant de un million cinq cent vingt-cinq mille (1.525.000) euros.

A cet égard, CertEurope déclare disposer d'une assurance professionnelle couvrant ses prestations de Certification électronique souscrite auprès de la compagnie HISCOX sous le numéro de police HA RCP0081352.

15 Coût du service

Le coût du SERVICE dépend des fournitures et des prestations demandées par l'ABONNE et il est communiqué par l'AE à l'ABONNE.

16 Propriété intellectuelle

Une licence individuelle d'exploitation non-exclusive est consentie à l'ABONNE pour toutes les fournitures, notamment les logiciels et la documentation. Les marques et les logos demeurent la propriété de leurs auteurs respectifs.

17 Durée du contrat

Le présent contrat prend effet à la date de l'émission du certificat pour une durée de **12** à **24** mois (durée de vie maximale de la bi-clé).

18 Réglementation et conformité

Le SERVICE fournit est conforme aux réglementations et normes suivantes :

- Le règlement européen eIDAS pour le niveau QCP-W – SSL de l'ETSI EN 319 411-2
- La dernière version des recommandations du CA/B Forum : EV SSL Certificate Guidelines https://cabforum.org/extended-validation/
- Les exigences du Référentiel Général de Sécurité (RGS) issues de l'Annexe A3 : Politique de Certification Type « certificats électroniques de services applicatifs » pour un usage d'authentification et/ou de signature au niveau * ou **.

19 Ensemble contractuel

Le contrat de service de Signature Electronique est constitué des présentes Conditions Générales et des Conditions Particulières à l'exception de tous autres documents échangés entre les parties.

20 Responsabilité de l'abonne

Les éléments confidentiels envoyés par voie postales par l'AC à L'Abonné transitent par le service courrier de l'Abonné sous son entière responsabilité.

21 Loi applicable et juridiction compétente

Le Contrat est régi par la loi française. Tout différend entre les Parties né de la formation, l'interprétation, l'exécution, la cessation ou la résiliation du Contrat fera l'objet d'une tentative de règlement amiable. A défaut, le différend sera porté devant le tribunal compétent de Paris, même en cas de pluralité de défendeurs ou d'appel en garantie.

Date

Signature de l'abonné