C@rteurope

CONTRAT D'ABONNEMENT AU SERVICE DE CERTIFICATION

Autorité de Certification
CERTEUROPE ADVANCED CA V4
Authentification Serveur

CONDITIONS GENERALES

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 DEFINITIONS

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.
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 : un 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.
FQDN (Fully qualified domain name) : 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.
Dispositif de protection des clés privées: Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en oeuvre 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 www.certeurope.fr/chaine-confiance-numerique.php. Ces conditions générales d'utilisation sont applicables aux profils de certificats dont les OID sont : 1.2.250.1.105.18.1.1.0 et 1.2.250.1.105.18.1.1.1 (authentification serveur SSL/TLS niveau*), 1.2.250.1.105.18.3.1.0 et 1.2.250.1.105.18.3.1.1 (authentification serveur SSL/TLS niveau**) et 1.2.250.1.105.18.4.1.0 et 1.2.250.1.105.18.4.1.1 (authentification serveur client).
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.
RGS : Référentiel Général de Sécurité mis en place par l'Administration française.
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 serveur**;

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 précédées de la mention "copie certifiée conforme à l'original").
- **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**.**

5 CONTROLES EFFECTUES AU COURS DE LA PROCEDURE 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.
- Pour un certificat authentification serveur SSL/TLS, il vérifie le FQDN.

Pour le niveau **, l'AE authentifie le RCAS lors d'un face-à-face physique en vérifiant sa pièce d'identité originale.

6 GENERATION ET DUREE DE VIE DU BI-CLE

Lors de la génération du certificat par l'AE, le bi-clé du certificat d'authentification serveur est généré par l'ABONNE. Le bi-clé tiré a une durée de vie maximum de 36 mois.

7 UTILISATION DES CERTIFICATS

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

- établissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager,
- établissement d'une session sécurisée entre un serveur et un agent,
- établissement 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, elles-mêmes issues de la Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

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 pendant 36 mois suivant son émission dans la limite de validité du bi-clé.

Les certificats ainsi que les LCR sont archivés par CertEurope pendant 10 ans à partir de leur génération.

Paraphes du RCAS

9 REVOCATION 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

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 ;
- 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 est publiée et accessible au public sur des serveurs disponibles 24 heures sur 24 et 7 jours sur 7.

10 OBLIGATIONS DE L'ABONNE

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

L'ABONNE a, de plus, 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

Le 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 :

- utiliser une méthode de transfert de la clé privée du certificat d'authentification serveur conforme aux exigences du RGS
- utiliser obligatoirement un boitier HSM qualifié au minimum au niveau standard par l'ANSSI (http://www.ssi.gouv.fr/) dans le cadre du RGS au niveau 2*
- mettre en œuvre un processus de désactivation de la clé privée du certificat d'authentification serveur conformément aux exigences du RGS
- mettre en œuvre un processus de destruction de la clé privée du certificat d'authentification serveur conformément aux exigences du RGS

12 DONNEES PERSONNELLES ET CONFIDENTIELLES

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

Les informations recueillies sont indispensables à CertEurope pour la mise en place et la gestion du service de certification électronique. Le représentant légal et le mandataire autorisent expressément CertEurope à traiter en mémoire informatisée les données les concernant conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée, et à les communiquer à ses sous-traitants ou à ses partenaires dans le respect des Conditions Générales du contrat d'abonnement au service de certification C@rteurope et de sa finalité. Le représentant légal et le mandataire peuvent, pour des motifs légitimes, s'opposer à ce que ces données fassent l'objet d'un traitement. Pour exercer leurs droits d'accès, de rectification ou d'opposition, le représentant légal et le mandataire doivent s'adresser par écrit à : CERTEUROPE Correspondant Informatique et Libertés 26 rue du Faubourg Poissonnière 75010 Paris

13 INFORMATION DE L'ABONNE

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 RESPONSABILITE 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 COUT DU SERVICE

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

16 RECLAMATIONS ET REGLEMENT DES LITIGES

Tous différends, découlant du présent contrat, peuvent être réglés par voie d'arbitrage si les parties au litige sont d'accord sur ce mode de règlement du conflit. Si tel est le cas, le règlement d'arbitrage est celui de l'ATA (Centre de conciliation et d'arbitrage des techniques avancées, 57, avenue de Villiers, 75017 Paris - Tél : 01 56 21 10 00 - Fax : 01 56 21 10 10 – http://www.legalis.net/ata), auquel les parties déclarent expressément se référer.
Si tel n'est pas le cas, les parties ont recours à la juridiction de droit commun, sachant que CertEurope attribue compétence au Tribunal de Grande Instance de Paris, à raison de son siège
Au besoin y compris par dérogation au règlement d'arbitrage de l'ATA, la sentence arbitrale sera susceptible d'appel devant les juridictions de droit commun.

17 PROPRIETE 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.

18 DUREE DU CONTRAT

Le présent contrat prend effet à la date de l'émission du certificat pour une durée de 36 mois (durée de vie maximale du bi-clé)

19 FORMALITES REGLEMENTAIRES

CERTEUROPE fait son affaire de toutes formalités administratives auprès de la DGME concernant le référencement de ses certificats pour permettre à l'ABONNE d'effectuer des téléprocédures en toute sécurité.
CERTEUROPE fait son affaire de toutes les formalités réglementaires prescrites par la réglementation nationale de la cryptographie.

20 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.

Signature du RCAS