certeurope
AN INFOCERT COMPANY

Convention d'enregistrement entre le Prestataire de Service de Confiance (PSCo) et l'Autorité d'Enregistrement (AE)

v20201125-01

Entre

CertEurope, 41 rue de l'Echiquier, 75010 Paris, société inscrite au registre du commerce de Paris sous le n° 434 202 180 représentée par Monsieur Guillaume Pyronnet, dûment habilité aux fins des présentes,

désignée ci-après par « CertEurope »,

ET

Organisme :

Adresse :

SIRET n°

représenté par

désigné ci-après par « Le Client »,

1 Objet

La présente convention décrit les conditions et modalités selon lesquelles « Le Client » exerce les fonctions d'enregistrement des Porteurs de certificats pour le compte de CertEurope.

Les fonctions d'enregistrement, assurées par « Le client », consistent en une suite d'opérations préalables et postérieures à l'obtention d'un certificat électronique par un Abonné et notamment une vérification administrative du dossier fourni par l'Abonné et une vérification de l'identité du Porteur en face-à-face.

CertEurope agit en tant que :

- ☑ Prestataire de service de confiance (PSCo)
- ☑ Autorité d'Enregistrement Technique (AET)

Le Client agit en tant que :

- ☐ Autorité d'enregistrement administrative (AEA)
- ☑ Autorité d'enregistrement déléguée (AED)
- ☐ Autorité d'Enregistrement Technique (AET)

La présente convention concerne les Autorités de Certification suivantes :

- ☑ CertEurope eID User
- ☐ CertEurope eID Corp
- ☐ CertEurope eID Website

2 Définitions

- **Abonné** : personne physique ou morale qui souscrit au service de Certification Electronique
- **Autorité d'Enregistrement (AE) :** 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 Administrative (AEA) :** fonction qui consiste à vérifier le dossier de demande de certificat.
  - **Autorité d'Enregistrement Technique (AET) :** fonction qui consiste à personnaliser (tirage du bi-clé et insertion du certificat) les clés des Porteurs.
  - **Autorité d'Enregistrement Déléguée (AED)** : fonction qui consiste à vérifier l'identité en face-à-face du Porteur ou du Mandataire de Certification.

  - L'AED fait signer un procès-verbal de face-à-face ou le cas échéant un procès-verbal de remise du support cryptographique au Porteur.
  - En cas de face-à-face avec le porteur, l'AED, après avoir vérifié la pièce d'identité originale du porteur, récupère une copie de celle-ci, la fait signer par le porteur et y porte sa signature.
- **Mandataire de Certification (MC) :** personne désignée par le représentant légal de l'entreprise pour effectuer les demandes de certificats et leurs révocations pour les membres de l'organisme. Si le MC procède à la vérification de l'identité du porteur en face-à-face en lieu et place de l'AED, il procède de la même façon que ce dernier.
- **Certificat électronique** : donnée électronique qui lie des données de vérification de signature à une personne identifiée.
- **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 PSCO).
- **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.
- **Opérateur :** personne physique assurant les fonctions de l'AEA, AET, AED
- **Politique de Certification (PC)** : ensemble de règles, identifié par un nom, qui définit le type d'applications auxquelles un certificat est adapté ou dédié.
- **Porteur** : personne physique titulaire du certificat électronique
- **Prestataire de service de certification électronique (PSCO) (également appelé "Autorité de Certification") :** personne morale qui délivre des certificats électroniques.
- **Révocation d'un certificat :** opération demandée par l'ABONNE ou toute autre personne autorisée à cet effet, par l'AEA ou directement par le PSCO et dont le résultat est la suppression de la garantie du PSCO sur un certificat donné, avant l'expiration de sa période de validité.
- **Bi-clé :** un bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaires à la mise en œuvre d'opérations de cryptographie basée sur des algorithmes asymétriques.
- **Données à Caractère Personnel :** désigne toute information relative à une personne physique, identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
- **Responsable du Traitement :** désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement.
- **Sous-Traitant :** s'entend au sens du RGPD et désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à Caractère Personnel pour le compte du Responsable du Traitement.
- **Traitement :** désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données à Caractère Personnel ou des ensembles de Données à Caractère Personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

3 Obligation des parties

Les obligations des parties dépendent de la répartition des rôles définie dans le chapitre OBJET.

3.1 Obligations de l'AEA

Les AEA mettent en œuvre les obligations identifiées dans la PC :

- Vérification des antécédents judiciaires des Opérateurs AEA avant l'attribution du rôle de confiance. L'entité responsable de l'AEA s'assure en permanence qu'aucun opérateur AEA n'est sanctionné pour une faute incompatible avec le rôle de confiance opérateur AEA ;
- Traitement des demandes de création de certificats émises par le Porteur, le Mandataire de Certification ou le Représentant Légal ;
- Vérification de l'exactitude des informations transmises au PSCO;
- Envoi des documents originaux fournis par les Porteurs (copie des Pièces d'identités, KBis, mandats, PV de remise…) au PSCO au moins une fois par mois.
- Protection de la clé privée de son certificat d'identification ;
- Restriction quant à l'utilisation de ses clés privées ;
- Protection de l'intégrité et la confidentialité des dossiers, de la remise par l'Abonné jusqu'à l'envoi au PSCO. Les transferts de dossier entre AED et AEA et entre AEA et PSCO, doivent se faire via un transporteur fiable et dans des conditions satisfaisantes en termes de confidentialité. Les dossiers doivent impérativement être stockés dans un lieu fermé à clé et protégé des accès frauduleux, des dégâts des eaux et des incendies potentiels.
- Protection de l'intégrité des supports cryptographiques des Porteurs lors des échanges avec les AED et l'AET.

Les obligations complémentaires suivantes sont à la charge des AEA **:**

- Respecter les relations contractuelles avec le PSCO,
- Se conformer au système de vérification de conformité mis en place par ce PSCO ;
- Rappeler aux Abonnés leurs obligations contractuelles

3.2 Obligations de l'AET

- Vérification des antécédents judiciaires des Opérateurs AET avant l'attribution du rôle de confiance. L'entité responsable de l'AET s'assure en permanence qu'aucun opérateur AET n'est sanctionné pour une faute incompatible avec le rôle de confiance opérateur AET ;
- Génération des certificats sur supports cryptographiques sur demande de l'AEA ;
- Révocation des certificats sur demande de l'AEA.
- Remise des certificats à l'AEA ou envoi au porteur si le face-à-face avec le porteur a eu lieu au dépôt du dossier de demande de certificat.
- Protection de l'intégrité des supports cryptographiques à destination des Porteurs. Les supports cryptographiques doivent impérativement être stockés dans un lieu fermé à clé.

3.3 Obligations de l'AED

Si le face-à-face est réalisé à la remise du certificat, l'AED doit :

- Assurer la protection des supports cryptographiques en sa possession contre le vol, la perte ou la détérioration ;
- Remettre le certificat en face-à face au Porteur ou aux personnes mandatées par l'Abonné sur présentation d'une pièce d'identité originale (carte nationale d'identité, passeport ou carte de séjour) ;
- Signer la photocopie de la pièce d'identité du Porteur. Si un MC a été désigné pour réaliser le face-à-face avec le Porteur, l'AED s'assure qu'une copie de la pièce d'identité du porteur signée par les parties, est retournée par le MC ;
- Faire signer au Porteur ou au Mandataire de Certification un Procès Verbal de remise de certificat ;

- Informer le Porteur sur l'usage du certificat (dépliant, adresse du site web …) ;
- Transmettre les preuves de la remise en face-à-face à l'AEA au moins une fois par mois.

Si le face-à-face est réalisé lors de la demande de certificat, l'AED doit :

- Vérifier l'identité du Porteur sur présentation d'une pièce d'identité originale (carte nationale d'identité, passeport ou carte de séjour) ;
- Signer la photocopie de la pièce d'identité du Porteur ;
- Délivrer une attestation de vérification d'identité ;
- Informer le porteur sur l'usage du certificat
- La photocopie de la pièce d'identité et l'attestation de vérification d'identité sont transmises à l'AEA soit par le porteur avec son dossier, soit par l'AED avec le dossier du porteur. Le face à face doit s'effectuer au maximum 1 mois avant la génération du certificat. Si le face-à-face est réalisé avec le MC, l'AED s'assure que le face-à-face entre le porteur et le MC a déjà eu lieu. Notamment, il s'assure qu'un PV de face-à-face signé par le MC et le porteur et qu'une copie de la pièce d'identité du porteur **s**ignée par les parties, sont présentes dans le dossier de demande de certificat.

3.4 Obligations du PSCo

Le PSCO met en œuvre les obligations identifiées dans la PC de référence en terme de :

- Création des certificats ;
- Révocation des certificats ;
- Fonctions de gestion des certificats ;
- Gestion des supports et données d'activation ;
- Protection de ses clés privées ;
- Restriction quant à l'utilisation de ses clés privées ;
- L'archivage des documents fournis par les Porteurs et transmis par l'AEA ;
- Mise en place d'audits de contrôles de conformité.

4 Responsabilite de l'Autorité d'Enregistrement Administrative

Il est expressément convenu entre les parties que l'AEA soussignée assume l'entière responsabilité de ses actes et omissions pour l'ensemble des tâches et diligences lui incombant, telles que décrites dans la présente convention.

En particulier, il est de la responsabilité de l'AEA de vérifier le K-bis ou l'avis SIRENE de l'entreprise du demandeur, l'identité et la qualité des personnes demandant la délivrance d'un certificat (cf. modalités en annexe I), de révoquer les certificats après connaissance de la cessation des fonctions des détenteurs, ou après connaissance d'une modification substantielle affectant la personnalité juridique du détenteur du certificat.

4.1 Fourniture des dispositifs d'enregistrement et des accessoires

Le PSCO met à la disposition de l'AEA un dispositif d'enregistrement d'Abonnés. Ce dispositif comprend :

- Un certificat électronique.
- Une interface en ligne pour commander des certificats
- Une interface en ligne pour traiter et suivre les commandes

Ce dispositif permet à l'AEA d'exercer ses fonctions d'enregistrement en liaison avec le PSCO et de communiquer avec ce dernier à l'aide de moyens de communication électroniques sécurisés.

Afin de permettre l'installation du dispositif matériel ou logiciel, l'AEA devra disposer d'un ordinateur répondant aux caractéristiques précisées dans le guide de formation des Opérateurs AE. Ces caractéristiques peuvent évoluer, suivant l'évolution des logiciels et du marché informatique.

4.2 Contenu des fonctions d'enregistrement

Les fonctions d'enregistrement exercées par l'AEA comprennent les prestations suivantes au bénéfice des Abonnés :

- Validation des demandes de certificat
- Organisation du face-à-face avec le porteur

Ces fonctions devront être assurées dans le respect des lois et règlements ainsi que des obligations générales de sécurité ci-dessous définies.

5 Responsabilité de l'autorité d'enregistrement administrative vis-à-vis de l'Autorité d'Enregistrement Déléguée

Il est expressément convenu entre les parties que l'AEA assume l'entière responsabilité des actes et omissions de l'AED pour l'ensemble des tâches et diligences lui incombant, telles que décrites dans la présente convention. En particulier, il est de la responsabilité de l'AEA de s'assurer que l'AED vérifie l'identité d'un Porteur en face-à-face et le cas échéant remette le certificat.

5.1 Contenu des fonctions de vérification d'identité

Les fonctions de vérification exercées par l'AED comprennent les prestations suivantes au bénéfice des Abonnés :

- Vérifier une pièce d'identité originale et valide du Porteur ou d'une personne mandatée par lui: carte nationale d'identité, passeport ou carte de séjour ;
- Effectuer une photocopie de la pièce d'identité et apposer la signature de l'Opérateur AED habilité ;
- Transmettre les éléments à l'AEA dans un délai maximum de un (1) mois

Ces fonctions devront être assurées dans le respect des lois et règlements ainsi que des obligations générales de sécurité ci-dessous définies.

5.2 Contenu des fonctions de remise du certificat

Si l'AED a en charge la remise du certificat, l'AED assure les prestations suivantes au bénéfice des Abonnés :

- Remise en main propre des moyens cryptographiques (clé USB ou carte à puce);

Ces fonctions devront être assurées dans le respect des lois et règlements ainsi que des obligations générales de sécurité ci-dessous définies.

5.3 Contenu des fonctions d'information

Les fonctions d'information exercées par l'AED comprennent les prestations suivantes au bénéfice des Abonnés :

- Fournir à l'Abonné une information sur l'utilisation du certificat (dépliant, adresse du site web, etc.) ;

6 Obligations générales de sécurité

Toutes les composantes de l'AE doivent respecter les règles de sécurité définies dans l'Annexe VI « Politique de Sécurité – environnement AE ».

7 Enregistrement

La phase d'enregistrement de l'Abonné incombe à l'AEA. Elle consiste pour l'AEA à recevoir du futur Abonné les informations relatives à ce dernier, à les vérifier, puis à les transmettre au PSCO.

La phase d'enregistrement est complétée par une phase particulière relative à la cryptographie au terme de laquelle l'AET procédera au tirage du bi-clé de l'Abonné.

Le détail des opérations de la phase d'enregistrement comme de l'étape cryptographique est donné dans l'Annexe I : « *Enregistrement de l'Abonné* ».

8 Demande de certificat

La demande de certificat est faite par une personne physique agissant pour le compte de la personne morale qu'elle représente ou qu'il lui a été permis de représenter. Un certain nombre d'informations et de pièces justificatives devra être fourni en soutien à la demande.

Le détail des opérations de la phase de demande de certificat par l'Abonné est donné dans l'Annexe II : *« Demande de certificat ».*

Après avoir effectué les contrôles nécessaires, l'AEA se charge de transmettre la demande de l'Abonné à l'AET pour obtention du certificat.

9 Remise du certificat

Après que l'AET a procédé à la confection du certificat, il le transmet sur le support cryptographique du Porteur à ce dernier par envoi postal avec remise contre signature si un face-à-face a déjà eu lieu, ou à l'AED (via l'AEA ou non) qui le remet ensuite au Porteur ou toute personne mandatée par lui.

Le détail des contrôles effectués pour la remise du certificat est donné dans l'Annexe II : « *Demande de certificat* ».

10 Révocation de certificat

Les demandes de révocation provenant du Porteur, du MC ou du Représentant légal de l'Abonné, doivent être redirigées vers les solutions de révocation proposées par le PSCO. :

- Par internet ou téléphone si le demandeur de la révocation dispose d'un code de révocation d'urgence
- En utilisant le formulaire disponible sur le site du PSCO, à retourner par courrier postal, signé et accompagné d'une copie de la pièce d'identité du demandeur de la révocation

Lorsque l'une des circonstances précisées dans l'Annexe III : « *Révocation de certificat* » se réalise, le certificat concerné doit être révoqué et placé par le PSCO dans une liste de certificats révoqués (LCR). Si la demande est justifiée, le PSCO révoque le certificat. L'Abonné titulaire du certificat est informé de la révocation par un récépissé envoyé à l'adresse « e-mail » du certificat.

11 Données à caractère personnel

CertEurope et le Client s'engagent à respecter, pour le Traitements de Données à Caractère Personnel relatif à la délivrance et à la gestion du cycle de vie des Certificats électroniques, les lois relatives à la

protection des Données à Caractère Personnel, notamment la loi n°78-17 du 6 janvier 1978 (ci-après « **Loi Informatique et Libertés** ») ainsi que le Règlement (UE) 2016/679 sur la protection des données (ci-après « **RGPD** »).

Dans le cadre de la présente convention, CertEurope en sa qualité d'Autorité de Certification (AC) agit en tant que de Responsable du Traitement.

Le Client, en sa qualité d'Autorité d'Enregistrement Administrative (AEA) et/ou d'Autorité d'Enregistrement Déléguée (AED), aura à traiter des Données à Caractère Personnel pour le compte du Responsable du Traitement.

11.1 Engagement des Parties

Les Parties s'engagent à traiter les Données à Caractère Personnel dans le respect du Contrat, et de la Politique de Certification et s'interdisent tout autre usage que ceux prévus par la présente convention. Les Parties s'engagent à traiter les Données à Caractère Personnel de manière loyale et licite, conformément aux principes prévus aux articles 5 et 6 du RGPD, et à préserver leur confidentialité.

11.1.1 Droit des personnes

L'exercice du droit des personnes concernées se fera directement auprès de l'AC.

L'AEA et/ou l'AED s'engage à porter assistance à CertEurope afin de lui permettre de répondre à toute demande d'exercice de droits par les personnes concernées, et/ou toute demande d'information émanant d'autorités de contrôle, administrations ou juridictions habilitées à formuler une telle demande.

L'AEA et/ou l'AED devra notamment, au plus tard dans un délai de dix (10) jours ouvrés à compter de la demande de l'AC, communiquer toutes les informations et réaliser toutes les actions permettant à l'AC de satisfaire à une demande d'exercice des droits émanant d'une personne concernée par le Traitement au titre des articles 12 à 20 du RGPD.

L'AEA et/ou l'AED s'engage à informer dans les meilleurs délais l'AC de toute demande qui lui serait adressée directement, et plus généralement de tout événement affectant le Traitement des Données à Caractère Personnel, et à l'informer expressément de toute demande émanant d'une personne concernée, ou d'une administration / juridiction habilitée à formuler une telle demande.

L'AEA et/ou l'AED s'interdit de communiquer directement des informations sur les Porteurs de Certificats électroniques à une administration / juridiction habilitée à formuler une telle demande et s'engage à rediriger toute demande de ce type vers l'AC.

11.1.2 Durée de conservation des Données à Caractère Personnel

Les Données à Caractère Personnel objets du Traitement sont traitées pour la durée prévue par la Politique de Certification, conformément aux règlementations applicables.

Au terme de la durée prévue par la Politique de Certification, les Parties s'engagent à détruire les Données à Caractère Personnel.

11.1.3 Sécurité

Les Parties s'engagent à prendre toutes précautions utiles, au regard de la nature des Données à Caractère Personnel et des risques présentés par le Traitement, pour préserver la sécurité des Données à Caractère Personnel et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Les Parties s'engagent dans ce cadre à mettre en place toutes mesures techniques et organisationnelles de sécurité et de confidentialité appropriées, à documenter et à pouvoir apporter la preuve de ces démarches.

Chaque Partie s'engage à veiller à ce que seuls ses personnels autorisés à traiter les Données à Caractère Personnel aux fins de l'exécution de la présente convention, y aient accès dans la stricte limite de ce qui est nécessaire à l'accomplissement de leurs fonctions, et à ce que ses personnels s'engagent à respecter la confidentialité des Données à Caractère Personnel.

11.1.4 Localisation des Données à Caractère Personnel

Chaque Partie confirme ne pas transférer, et veille à ce que ses éventuels Sous-Traitants ne transfèrent pas non plus de Données à Caractère Personnel vers un pays tiers hors UE, ne bénéficiant pas de décision d'adéquation telle que prévue par l'article 45 du RGPD.

11.1.5 Sous-traitance

L'AEA et/ou l'AED n'utilise aucun Sous-Traitant dans le cadre de son rôle d'Autorité d'Enregistrement Administrative (AEA) ou déléguée (AED), sans autorisation écrite préalable de l'AC.

L'AEA et/ou l'AED s'engage à imposer par contrat à ses éventuels Sous-Traitants les mêmes obligations en matière de protection de Données à Caractère Personnel que celles fixées par le présent article. L'AEA et/ou l'AED s'engage notamment à assurer à l'autre Partie que ses Sous-Traitants présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées et conformément au RGPD et à la Loi Informatique et Libertés.

Chaque Partie reconnait être pleinement responsable vis-à-vis de l'autre Partie si ses Sous-Traitants ne remplissent pas leurs obligations en matière de protection de Données à Caractère Personnel.

11.1.6 Notifications en cas de violation des Données à Caractère Personnel

En cas d'incidents ou de violation de Données à Caractère Personnel, affectant le Traitement, Chaque Partie s'engage à informer l'autre Partie dans les quarante-huit (48) heures ouvrées après en avoir pris connaissance, et à prendre toutes mesures correctives appropriées. La Partie concernée s'engage notamment à communiquer dans les meilleurs délais à l'autre Partie tous les éléments dont elle dispose concernant les conditions entourant l'incident de sécurité, dont notamment la nature et l'étendue des Données à Caractère Personnel impactées, le nombre de personnes concernées, les conséquences probables et les conditions techniques dans lesquelles l'incident a eu lieu.

L'AEA et/ou l'AED s'interdit de communiquer des informations concernant une violation de Données à Caractère Personnel au public, à l'autorité de contrôle ou à un quelconque tiers. L'AC, en sa qualité d'Autorité de Certification conserve la responsabilité exclusive de telles communications et notifications.

11.1.7 Accompagnement

Chaque Partie s'engage à intégrer à son registre le Traitements effectué dans le cadre de la présente convention.

L'AEA et/ou l'AED s'engage à mettre à disposition de l'AC tous les éléments nécessaires pour démontrer le respect des obligations prévues par toutes lois et textes en vigueur relatifs à la protection des Données à Caractère Personnel et prévues au présent article.

L'AEA et/ou l'AED informera immédiatement l'AC, selon lui, une instruction ou une action constitue une violation du RGPD ou d'autres dispositions des lois et règlementations applicables et relatives à la protection des Données à Caractère Personnel.

L'AEA et/ou l'AED s'engage à fournir toute assistance raisonnable à l'AC dans le cadre d'éventuelles analyses d'impact relatives à la protection des Données à Caractère Personnel, ou dans le cadre de procédures menées par une autorité de contrôle.

Enfin, l'AEA et/ou l'AED s'engage à informer sans délai l'AC en cas de contrôle de la CNIL, ou de toute autorité administrative ou judiciaire, concernant le Traitement de Données à Caractère Personnel mis en œuvre dans le cadre de l'exécution de la présente convention.

11.2 Informations relatives au Traitement

11.2.1 Finalités du Traitement

Enregistrement des demandes de certificats électroniques,

11.2.2 Catégories de Personnes Concernées

Porteurs de Certificats, Mandataires de Certification, représentant légaux des entités demandant des certificat (Clients et/ou salariés de l'Autorité d'Enregistrement).

11.2.3 Catégories de Données à Caractère Personnel traitées

- Données relatives à l'identité des personnes concernées.
- Coordonnées des personnes concernées.

11.3 Désignation d'un DPO

L'AC déclare disposer d'un Délégué à la Protection des Données (« DPO »), en charge des questions relatives aux Données à Caractère Personnel objets du Traitement. Le DPO veillera à ce que les Traitements de Données à Caractère Personnel effectués dans le cadre du Contrat soient conformes à la Loi Informatique et Libertés/au RGPD.

Le DPO est joignable sur privacy@certeurope.com

L'AEA et/ou l'AED s'engage à communiquer à l'AC les coordonnées de son DPO et/ou de la personne en charge de la protection des Données à Caractère Personnel. A défaut, les notifications, communications et autres alertes seront envoyées par l'AC aux opérateurs AEA désignés en annexe de la présente convention.

12 Journalisation des évènements

Toutes les opérations électroniques effectuées par l'AEA ou l'AET sont journalisées automatiquement par le PSCO avec les éléments d'authentification des Opérateurs et d'horodatage afin d'être en mesure de fournir une preuve en justice.

L'Annexe IV : *« Journalisation et archivage »* précise notamment :

- Les éléments à mémoriser pour chaque événement, l'environnement d'exploitation et les événements techniques, les demandes et opérations relatives aux certificats,
- Les modalités de journalisation, la rédaction et la conservation du journal

13 Vérification de conformité des prestations

Le PSCO exerce son contrôle sur chacun de ses composants par le biais d'une commission de suivi. Chaque composante (AEA, AET et AED) devra :

- se soumettre aux contrôles de conformité effectués par l'auditeur du PSCO
- respecter les conclusions et remédier aux non-conformités révélées directement par un contrôle de l'auditeur du PSCO.

14 Durée

La convention est conclue pour une durée de un (1) an et sera reconduite tacitement sauf dénonciation par l'une ou l'autre des parties et par lettre recommandée avec accusé de réception à l'échéance de la convention en respectant un préavis de trente (30) jours.

15 Rupture de la convention

La présente convention sera résiliée de plein droit si au cours de son exécution, l'une ou l'autre des parties ne respecte pas ses obligations contractuelles et n'apporte pas remède à son manquement dans les trente jours de la réception de la lettre recommandée avec accusé de réception adressée par l'autre partie.

La rupture de la convention sera signifiée par la partie concernée ou par la partie la plus diligente après l'envoi d'une mise en demeure restée sans effet plus d'un mois et ce, sans préjudice de tous dommages et intérêts.

16 Ensemble contractuel

La convention est formée de l'ensemble des présentes et de ses annexes :

- Annexe I : « Enregistrement de l'Abonné »
- Annexe II : « Demande de certificat »
- Annexe III : « Révocation de certificat »
- Annexe IV : « Journalisation et archivage »
- Annexe V : « Signatures des Opérateurs »
- Annexe VI : « Politique de Sécurité »

Les annexes énoncées ci-dessus reprennent succinctement les éléments présents dans le document de référence de l'ICP : la Politique de Certification disponible sur le site www.certeurope.fr rubrique « Chaine de confiance ».

17 Dispositions diverses

Si une disposition de la présente convention venait à être tenue pour nulle et non avenue du fait de l'application d'une loi ou d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres dispositions garderont toute leur force et leur portée.

Tout différend, découlant du présent contrat, sera dénoué par voie d'arbitrage, suivant le règlement d'arbitrage de l'ATA (Centre de conciliation et d'arbitrage des techniques avancées, 57, avenue de Villiers, 75017 Paris) auquel les parties déclarent expressément se référer. Au besoin y compris par dérogation au règlement d'arbitrage, la sentence arbitrale sera susceptible d'appel.

Le fait pour l'une des parties aux présentes de ne pas se prévaloir de toute ou partie des dispositions des présentes ne peut en aucun cas être assimilé à une renonciation tacite à ce droit.

Fait à ……, le ……. / ……../……

Pour le PSCo

Pour L'Autorité d'Enregistrement

Annexe 1 : Enregistrement de l'abonné

Vérification de l'identité de l'organisation

L'AEA vérifie l'identification de l'organisation, de son représentant légal et de toute personne désignée par ce dernier, directement ou indirectement, pour le représenter. A défaut de désignation d'un Mandataire de Certification, le représentant légal est l'unique représentant de l'organisation.

Lors de l'enregistrement, l'AEA doit vérifier l'existence de l'organisation, l'identité de son représentant légal grâce aux documents fournis comme justificatifs. L'organisation doit apporter pour sa part la chaîne des mandats conférant leur pouvoir aux Mandataires de Certification.

Vérification de l'identité des Abonnés

L'AEA acceptera seulement les demandes de certificat appuyées par des dossiers constitués de pièces justificatives fiables.

Pour toute demande de certificat faite au titre de l'appartenance à une organisation, il faut que ladite demande soit confirmée par écrit par un Mandataire de Certification ou le représentant légal.

L'AEA doit conserver les pièces reçues pour l'enregistrement de l'Abonné, examiner les pièces et documents remis avec un soin raisonnable et vérifier s'ils présentent ou non l'apparence de conformité et de validité.

S'il s'agit du porteur, avant la distribution, l'AEA, ou une personne mandatée par elle comme l'AED (collaborateur ou société sous contrat pour procéder à l'installation du certificat chez l'Abonné), vérifie en face à face, c'est-à-dire en présence du porteur, un original d'une pièce d'identité officielle du porteur comportant sa photo et sa signature ;

S'il s'agit du Mandataire de Certification, avant la distribution, l'AEA, ou une personne mandatée par elle comme AED (collaborateur ou société sous contrat pour procéder à l'installation du certificat chez l'Abonné), vérifie en face à face, c'est-à-dire en présence du Mandataire de Certification, un original d'une pièce d'identité officielle du Mandataire de Certification comportant sa photo et sa signature. Le Mandataire de Certification, s'il réalise le face-à-face avec l'AEA, a par la suite la charge de réaliser le face-à-face avec le porteur, dans les conditions du paragraphe précédent.

Annexe 2 : Demande de Certificat

Origine de la demande

Un certificat est demandé par le représentant légal, un Porteur autorisé par le représentant légal ou un Mandataire de Certification.

Si le Porteur n'est pas le représentant légal, il doit exister une autorisation du représentant légal ou d'un Mandataire de Certification identifié. Dans tous les cas le contrat devra être signé par le Porteur du certificat.

Si un Mandataire de Certification est désigné, la procuration doit faire mention des obligations du Mandataire de Certification.

L'AEA acceptera seulement les demandes de certificat appuyées par des dossiers constitués de pièces justificatives fiables avec les informations décrites ci-dessous.

Informations à fournir

Pour une demande de certificats RGS**, les informations suivantes doivent figurer dans la demande de certificat d'Abonnés :

- Un contrat d'abonnement signé par l'Abonné
- Le cas échéant, une autorisation de demande de certificat portant le numéro SIREN de l'entreprise, signée par le représentant légal ou le Mandataire de Certification,
- Le cas échéant, la désignation du Mandataire de Certification signée par le représentant légal avec cachet de l'entreprise.
- un justificatif d'identité en cours de validité du représentant légal sous la forme de copies de documents d'identification (photocopie du passeport, photocopie de la carte nationale d'identité, etc.) ;
- une déclaration de l'Abonné, portant l'acceptation des engagements de l'Abonné et désignant éventuellement le Mandataire de Certification pour le représenter auprès de l'AEA et lui remettre le certificat ;
- une adresse postale de l'Abonné ;
- un justificatif d'identité en cours de validité de l'Abonné sous la forme de copies de documents d'identification (photocopie du passeport, photocopie de la carte nationale d'identité, etc.) ;
- le nom d'Abonné à utiliser dans le certificat ;
- l'adresse de courrier électronique du demandeur.

Ces informations peuvent évoluer conformément aux règlementations en vigueur, notamment aux évolutions du RGS et de la Politique de Certification.

Opérations à effectuer

Lors d'une demande de certificat, l'AEA doit effectuer les opérations suivantes :

- établir l'identité du demandeur, en vérifiant les pièces justificatives présentées par l'Abonné ou le Mandataire de Certification ;
- vérifier le cas échéant l'identité du représentant légal ou du mandataire ;
- s'assurer que le demandeur a pris connaissance des modalités applicables pour l'utilisation du certificat ; l'AEA vérifie la date et la signature par le Porteur du contrat ou de la déclaration indiquant qu'il a pris connaissance de ses droits et obligations ;
- demander à l'AET la génération du certificat sur support cryptographique ;
- réceptionner le support cryptographique ;
- le cas échéant, remettre en face à face contre récépissé de certificat à l'Abonné.

Emission du Certificat

L'émission d'un certificat n'interdit en aucune façon au PSCO de le révoquer ultérieurement, s'il estime qu'il a été demandé dans de mauvaises conditions.

L'émission d'un certificat par le PSCO indique que celui-ci a définitivement et complètement approuvé la demande de certificat.

A la réception d'une demande de certificat :

- Le PSCO doit s'assurer que la demande a bien été émise par l'AEA qu'elle a reconnue et que l'AEA a traité la demande, et fournit une trace imputable de son avis ;
- Le PSCO doit générer le certificat ;
- Le PSCO doit notifier à l'Abonné la mise à disposition de son certificat et l'ensemble des procédures à suivre pour être en mesure de l'obtenir et de l'utiliser en cas d'acceptation ;
- L'AEA doit mettre le certificat à disposition de l'Abonné, c'est à dire rendre accessible par des moyens physiques ou logiques les informations permettant l'obtention du certificat.

Face-à-face

Lors du face-à-face avec l'AE, le Porteur doit communiquer une copie de sa pièce d'identité, sur laquelle sera apposée sa signature manuscrite que l'AE contresignera également.

Dans le cas où le face-à-face se déroule avec le MC, ce dernier remettra à l'AE la copie de la pièce d'identité du Porteur qu'il représente, sur laquelle sera apposée la signature manuscrite du Porteur. Ce document sera également contresigné par le MC avant remise à l'AE.

Acceptation du certificat

Les modalités de vérification et d'acceptation du certificat sont décrites dans la Politique de Certification.

Annexe 3 : Révocation de Certificat

Causes possibles de révocation

Lorsque la confiance en la clé privée d'un Abonné n'est, pour des raisons objectives, plus assurée, le certificat concerné doit être révoqué et placé dans une liste de certificats révoqués (LCR).

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat :

- fin du contrat de travail du Porteur (ex : démission ou cessation de ses fonctions, licenciement ou révocation, décès) ;
- non renouvellement du contrat par l'Abonné à la date anniversaire
- suspicion de compromission, compromission, perte ou vol de la clé privée ou des données d'activation ;
- modification de la situation de l'Abonné remettant en cause l'exactitude des informations contenues dans le certificat ;
- les informations sur le Porteur figurant dans son certificat (hormis l'adresse email) ne sont plus en cohérence avec l'utilisation prévue du certificat et ce, avant l'expiration normale du certificat ;
- suspicion de compromission, compromission, perte ou vol de la clé privée du PSCO, ou plus généralement, révocation du certificat du PSCO;
- décision de changement de composante du PSCO ou de l'AE suite à non-conformité des procédures de la DPC ;
- cessation d'activité de l'organisme porteur du certificat ou modification substantielle de sa situation juridique ;

Outre les cas de révocation de certificats mentionnés plus haut, l'AEA et le PSCO doivent respectivement demander la révocation ou révoquer un certificat dès lors qu'ils sont en possession d'informations de nature à indiquer une perte de confiance dans un certificat.

Plus généralement, l'AEA et le PSCO peuvent respectivement et à leur discrétion, demander la révocation ou révoquer le certificat d'une entité identifiée lorsqu'elle ne respecte pas les obligations énoncées dans la Politique de Certification et dans tous documents contractuels ainsi que dans toute loi et règlement applicable.

Personnes pouvant demander une révocation

Seuls peuvent demander la révocation d'un certificat (certificat d'Abonné ou d'une composante de l'ICP) :

- l'Abonné;
- le Porteur
- le Mandataire de Certification ;
- le représentant légal ;
- le PSCO;
- l'AEA.

Procédure de demande de révocation

L'AEA ou le PSCO doit s'assurer que lors de la demande de révocation, toutes les procédures et exigences publiées par le PSCO sont respectées.

Dans le cas où son certificat se doit d'être révoqué, l'Abonné doit informer au plus vite le PSCO. L'Abonné ne pouvant plus s'authentifier au moyen de son certificat, le PSCO authentifiera la demande de révocation :

- soit au moyen d'une signature numérique valide reconnue par le PSCO (par exemple, celle du Mandataire de Certification pour le certificat d'Abonné agissant pour le compte d'une organisation) ;
- soit au moyen d'un code de révocation d'urgence fournit à l'Abonné ou défini par lui-même.

Dans tous les cas, la demande de révocation doit contenir explicitement les informations d'identification de l'Abonné et de son certificat. La demande doit également contenir, quand c'est possible, la cause de révocation et, le cas échéant, les éléments justificatifs de cette cause.

Les causes de révocation mentionnées dans les certificats révoqués ne doivent en aucun cas contenir d'informations privées sur les personnes et ce conformément aux lois nationales.

Si la procédure de demande de révocation d'un certificat est justifiée et acceptée, la révocation est déclenchée. L'ensemble des opérations et des mesures prises par le PSCO est consigné et archivé.

L'AET peut, sur demande de l'AEA, procéder directement à la révocation via l'interface fournie par le PSCO à cet effet. Les éléments justificatifs (courrier de demande) seront transmis pour archivage au PSCO.

Dans tous les cas de révocation d'un certificat, l'Abonné doit être informé de la révocation de son certificat. Cette notification doit indiquer la date à laquelle la révocation du certificat a pris effet et peut être effectuée par messagerie électronique.

Temps de traitement d'une demande révocation

A la réception d'une demande de révocation, en provenance de l'Abonné ou du Mandataire de Certification, le PSCO analyse cette demande en vérifiant l'authenticité du demandeur puis analyse les causes et justificatifs éventuels de révocation. Si la demande comporte toutes les informations nécessaires à l'authentification du demandeur et si les motifs correspondent à l'un des motifs décrits ci-dessus, le PSCO révoque le certificat en faisant introduire le numéro de série du certificat et éventuellement d'autres informations dans une liste de révocation.

Les demandes de révocation doivent être traitées immédiatement à réception de la demande.

Le PSCO sera immédiatement informé en cas de compromission avérée ou soupçonnée de la clé d'une des composantes de l'ICP. Pour tous les autres cas de révocation, le temps de traitement, incluant la publication, ne devra pas dépasser 24h.

La prise en compte des demandes de révocation par le service de révocation du PSCO doit être effective 24h/24 et 7j/7.

Annexe 4 : Journalisation et Archivage

Types de données à archiver

Les données archivées par les AEA sont les suivantes :

- Un exemplaire de la présente convention qui la lie avec le PSCO
- Une copie (papier ou électronique) des données d'enregistrement (dossiers de demande de certificat),

Les données archivées par le PSCO et transmises par l'AEA (*) sont les suivantes :

- les justificatifs d'identité des Abonnés
- le contrat signé par les Abonnés, les Clients et les Mandataires de Certification,
- les données d'enregistrement telles que décrites en Annexe 2.
- les demandes de révocation

(*) L'AEA transmet au PSCO au moins une fois par mois les documents (dossiers originaux) fournis par les porteurs de certificat.

Période de rétention des archives

La durée d'opposabilité des documents concernant les Abonnés étant de 7 ans après expiration du certificat et la période de rétention des archives est la suivante :

les justificatifs d'identité des Abonnés	7 ans après expiration du certificat
le contrat signé par les Abonnés, les Clients et les Mandataires de Certification	7 ans après expiration du certificat
les données d'enregistrement/renouvellement telles que décrites dans la PC de référence	7 ans après expiration du certificat

Protection des archives

Pendant tout le temps de leur conservation, les archives doivent :

- être protégées en intégrité ;
- être protégées des accès frauduleux ou par des personnes non-autorisées
- être disponibles ;
- pouvoir être relues et exploitées.

Procédures de copie de récupération des archives

Il appartient contractuellement aux AEA de s'assurer de la disponibilité des copies d'archives (papier ou électronique) des dossiers de demande de certificat transmis au PSCO. Ces éléments pourront être conservés par tous moyens à leur convenance.

Une archive doit être récupérable sous un délai inférieur à 2 jours ouvrés auprès du PSCO.

Annexe 5 : Signatures des opérateurs

Liste des personnes physiques réalisant en pratique les tâches de l'Autorité d'Enregistrement Administratives

Les signataires s'engagent à respecter les obligations contenues dans la convention AC – AEA. Notamment, ils s'engagent à fournir à leur employeur un bulletin de casier judiciaire n°3 avant leur prise de fonction.

Prénom Nom	**Fonction AEA/AET/AED**	**Date**	**Signature**

Annexe 6 : Politique de sécurité certeurope pour les autorités d'enregistrement

Document disponible auprès de CertEurope sous la référence « Politique de Sécurité – environnement AE ».