INFRASTRUCTURE DE CONFIANCE NATIONALE
AC ENTREPRISES
CONDITIONS GENERALES D'UTILISATION

État du document - Classification	Référence
En cours - Publique	2.16.492.1.1.1.1.4.3

Version	Date	Description
1.0	16/03/2021	Version initiale
2.0	04/11/2021	Version modifiée
2.2	04/03/2022	Version modifiée
2.3	29/11/2022	Version modifiée
2.4	29/06/2023	Version modifiée

Table des matières

1 OBJET

Les présentes Conditions Générales d'Utilisation (ou « Conditions Générales d'Utilisation du certificat », ci-après désignées « CGU ») ont pour objet de préciser les modalités de délivrance et d'utilisation des certificats électroniques de signature électronique, d'authentification et de cachet électronique proposés par la Direction du Développement Économique(ci-après désignée « DDE») ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les présentes CGU s'appliquent à tout Demandeur sollicitant les certificats électroniques proposés par la DDE et utilisant lesdits certificats.

Le Porteur, respectivement le Responsable du Certificat confirme avoir lu et compris l'intégralité des présentes CGU avant toute utilisation de Certificat et s'engage à les respecter.

2 DEFINITIONS

Les mots et expressions ci-après commençant par une lettre majuscule, au singulier ou au pluriel, sont employés dans les présentes avec la signification suivante :

- **Autorité de Certification ou AC** : désigne l'ensemble des systèmes informatiques qui permettent de créer et révoquer des certificats électroniques.
- **Autorité d'Enregistrement ou AE** : désigne la DDE.

Elle assure les fonctions suivantes :

- Réception des dossiers de demande de génération d'un certificat ;
- Réception des dossiers de demande de révocation d'un certificat ;
- Vérification de l'identité et de l'habilitation du Demandeur de certificats ;
- Remise au futur porteur, RC le cas échéant, des supports cryptographiques pour utiliser les certificats correspondants
- Remise au futur RC des certificats de cachet correspondants ;
- Déclenchement de la génération des certificats ;
- Traitement de la révocation des certificats ;
- Déclenchement des fonctions d'archivage des données.
- **Certificat** : désigne la Clé publique d'un Porteur, respectivement d'un Responsable du Certificat, à laquelle sont associées d'autres informations. Elle correspond à la clé privée délivrée par l'autorité de certification.
- **Conditions Générales d'Utilisations ou CGU** : désigne les présentes CGU.
- **Contrat** : ensemble contractuel constitué des présentes CGU, du dossier de demande de certificat ainsi que de la Politique de Certification afférents figurant à l'adresse suivante : https://spe.gouv.mc/entreprises applicables à la date de conclusion du contrat.
- **C2SC** : Comité de Suivi des Services de Confiance.
- **Demandeur** : Le Demandeur est la personne physique qui effectue une demande auprès d'une Autorité d'Enregistrement pour obtenir un certificat de personne physique ou de cachet.
- **Données à caractère personnel / Données personnelles / Informations nominatives** : toute information se rapportant à une personne physique identifiée ou identifiable (« personne

concernée »). Est réputée être une « personne physique identifiable » toute personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité.

- **Infrastructure de Confiance Nationale ou ICN** : L'ICN est l'ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance mise en œuvre par l'AMSN pour le compte du Gouvernement princier. L'AC ENTREPRISES est une des autorités rattachées à l'ICN.
- **Mandataire de certification** : désigne la personne physique ayant reçu mandat du représentant légal pour gérer la flotte de certificats de l'entreprise pendant leurs cycles de vie (processus d'enregistrement comprenant le contrôle du dossier et de l'identité du porteur, processus de renouvellement et de révocation …). Il peut s'agir d'un tiers (comme par exemple un cabinet d'avocat ou un commissaire aux comptes) dont la responsabilité est engagée à travers une relation contractuelle avec l'entreprise qui l'habilite à la représenter. Le représentant légal est mandataire de certification par défaut.
- **Officier de sécurité de l'ICN** : Personne qui a pour mission, sous les ordres de son autorité d'emploi, de fixer les règles et les consignes de sécurité à mettre en œuvre relatives aux personnes et aux informations ou supports protégés et d'en vérifier l'exécution.
- **Opérateur d'enregistrement** : désigne l'opérateur de la DDE en charge du traitement des dossiers de demande de certificats.
- **Politique de Certification ou PC** : la PC de l'AC Entreprises désigne le document établissant les principes qui s'appliquent à l'AC, aux personnes morales, aux Représentants légaux, aux Mandataires de certification et aux porteurs, respectivement aux RC, intervenant dans l'ensemble du cycle de vie d'un certificat, (consultable à l'adresse suivante : https://spe.gouv.mc/entreprises)

  Les identifiants des PC applicables pour les présentes CGU sont :
  - La PC de l'AC Racine : 2.16.492.1.1.1.1.1.1 ;
  - La PC de l'AC Entreprises : 2.16.492.1.1.1.1.4.1
- **Porteur** : désigne le Porteur de certificat, personne physique identifiée dans le certificat.
- **Processus d'enregistrement** : désigne le processus d'enregistrement qui consiste à créer et gérer le dossier de demande de certificat.
- **RCI** : Le Répertoire du Commerce et de l'Industrie (RCI) répertorie officiellement les activités commerciales, les sociétés autres que les sociétés civiles et les groupements d'intérêt économique. Il est consultable au lien suivant : https://www.rci.gouv.mc/rc/.
- **Représentant légal** : désigne la personne (ou des personnes) légalement désignée(s) en vue de représenter l'entreprise. Il s'agit de la personne (ou des personnes) désignée(s) dans les statuts de l'entreprise et dont son (leurs) nom(s) est (sont) renseigné(s) dans le Répertoire du Commerce et de l'Industrie (RCI).
- **Responsable du Certificat de la personne morale ou RC** : La notion de Responsable de Certificat ne s'applique qu'aux certificats finaux de personnes morales. Le Responsable du Certificat est la personne physique nommée et mandatée par le Responsable Légal de la personne morale pour gérer tout ou partie des certificats de cachet de cette dernière.

3 POINT DE CONTACT

Les demandes d'informations relatives à la délivrance des certificats électroniques proposés par la DDE peuvent être réalisées :

- Par courrier postal : Direction du Développement Économique- 9 rue du Gabian, MC 98000 MONACO
- Par e-mail : esign@gouv.mc.

4 TYPES DE CERTIFICAT ET USAGES

Les types de Certificats délivrés sont les suivants :

- Les Certificats permettant la signature électronique d'une personne physique représentant une personne morale ;
- Les Certificats de cachet pour le compte de personnes morales qui pourront être délivrés par email (cachet serveur) ou sur une carte à puce (cachet sur carte à puce) ;
- Les Certificats d'authentification d'une personne physique représentant une personne morale qui permettront dans de futurs usages à la personne physique de s'authentifier sur les téléservices de l'Administration.

Les types de Certificats et usages sont décrits dans la PC de l'AC Entreprises (consultable à l'adresse suivante : https://spe.gouv.mc/entreprises).

Des notifications sont réalisées sur le site de référence mconnect.gouv.mc en cas de problèmes susceptibles de porter atteinte à l'intégrité et la disponibilité du service.

5 LIMITE D'USAGE

Les Porteurs, respectivement les RC, doivent respecter strictement les usages autorisés des bi-clés et des Certificats. Dans le cas d'une utilisation frauduleuse, leur responsabilité peut être engagée.

L'usage autorisé de la bi-clé et du Certificat associé est précisé dans le Certificat lui-même.

L'utilisation de la clé privée du Porteur, respectivement du RC, et du Certificat associé est strictement limitée au service défini par l'identifiant de sa PC.

Le Porteur, respectivement le RC, reconnait être informé qu'une utilisation frauduleuse ou non conforme aux présentes CGU ainsi qu'à l'usage autorisé de la bi-clé et du Certificat est un motif légitime de révocation par l'AC.

L'usage des Certificats est limité aux usages décrits dans la PC de l'AC Entreprises consultable à l'adresse suivante : https://spe.gouv.mc/entreprises.

6 CONDITIONS D'OBTENTION ET D'UTILISATION DU CERTIFICAT

6.1 DEMANDE DE CERTIFICAT ET JUSTIFICATIFS A FOURNIR

Le service d'enregistrement proposé par l'AC ENTREPRISES est disponible, sur rendez-vous, pendant les heures d'ouverture de la section du RÉPERTOIRE DU COMMERCE ET DE L'INDUSTRIE.

Une demande de Certificat doit être faite auprès de l'AE par l'intermédiaire d'un dossier d'enregistrement.

Le Processus d'enregistrement consiste à créer puis instruire le dossier de demande de Certificat.

Deux canaux d'enregistrement sont possibles :

- par voie dématérialisée, via le dépôt du dossier d'enregistrement dématérialisé au travers d'un formulaire en ligne accessible depuis un téléservice,
- par voie papier, via le dépôt du dossier d'enregistrement au format papier auprès d'un Opérateur d'Enregistrement. Cette solution dite de repli ne sera mise en œuvre qu'en cas de problème avec le téléservice.

6.1.1 Au travers du téléservice

Le Demandeur a la possibilité de déposer un dossier d'enregistrement par voie dématérialisée via le téléservice « Obtenir un certificat de signature ou de cachet électronique professionnel », disponible à l'adresse : https://teleservice.gouv.mc/ecertificats-pro/.

Les informations suivantes sont demandées dans le formulaire en ligne :

- Informations sur l'organisation concernée par la(es) demande(s) de certificat(s) ;
- Informations personnelles du/des représentant(s) légal(aux) ;
- Questions de sécurité du/des représentant(s) légal(aux) ;
- Informations concernant les certificats demandés ;
- Informations personnelles du ou des porteur(s)/responsable(s) de certificat ;
- Questions de sécurité du ou des porteur(s)/responsable(s) de certificat ;
- Informations personnelles du mandataire de certification (le cas échéant) ;
- Questions de sécurité du mandataire de certification (le cas échéant).

Le Demandeur atteste ensuite avoir pris connaissance du caractère payant de la demande de délivrance de certificat, afin de poursuivre la démarche.

Une copie numérique des pièces justificatives suivantes sont demandées dans le cadre d'une demande :

- Justificatif d'identité du/des représentant(s) légal(aux) ;
- Attestations concernant le(s) porteur(s)/responsable(s) de certificat ;
- Justificatif d'identité du ou des porteur(s)/responsable(s) de certificat ;
- Justificatif d'identité du mandataire (le cas échéant) ;
- Mandat du mandataire de certification (le cas échéant) ;
- Engagement du mandataire (le cas échéant).

Le justificatif comportant les attestations relatives à un porteur/responsable de certificat ainsi que l'engagement du mandataire de certification, le cas échéant contiennent l'acceptation des présentes CGU

par toutes les parties prenantes, ainsi que les signatures manuscrites voire électroniques, lorsque cela est possible.

Note : pour le cas des associations, fédérations et professions libérales, le Demandeur est notifié que des documents complémentaires pourront lui être demandés dans le cadre de l'instruction de son dossier d'enregistrement.

Le dossier d'enregistrement est ensuite transmis par voie dématérialisée à un outil de traitement. Un Opérateur d'enregistrement prend en charge le dossier au travers de cet outil et analyse sa recevabilité.

Dans tous les cas, le Demandeur est notifié par courriel et un document justificatif de décision détaillant les étapes de l'instruction est mis à sa disposition dans son interface du téléservice.

Si le dossier est recevable, l'Opérateur d'enregistrement prend contact avec le Demandeur en dehors du téléservice (téléphone ou courriel) afin de convenir d'un rendez-vous au sein de la Direction du Développement Économique pour finaliser la demande et délivrer les certificats.

Lors du rendez-vous, la personne se déplaçant au guichet (représentant légal, porteur/responsable du certificat ou mandataire de certification) doit produire les documents suivants :

- Une pièce d'identité en cours de validité la concernant ;
- L'original du document concernant les attestations relatives au porteur, respectivement au responsable de certificat ;
- L'original du mandat du mandataire de certification, le cas échéant ;
- L'original de l'engagement du mandataire de certification, le cas échéant.

Il est précisé que les justificatifs valablement signés électroniquement avec un certificat de signature électronique reconnu à valeur probante sur le territoire de la Principauté et fournis au travers du téléservice n'ont pas à être déposés au guichet au format papier avec signature manuscrite.

La demande est tracée et conservée pendant dix (10) ans après production du ou des certificat(s) attenant(s).

6.1.2 Au travers de formulaires papiers

Trois processus d'enregistrement sont possibles :

- Processus d'enregistrement d'un Porteur, respectivement d'un RC, qui réalise le processus pour lui-même.
- Processus d'enregistrement des Mandataires de certification, qui habilite une personne à réaliser ces processus d'enregistrement pour les Porteurs, respectivement les RC, d'une entreprise.
- Processus d'enregistrement d'un Porteur, respectivement d'un RC, réalisé par un Mandataire de certification.

L'enregistrement nécessite une prise de rendez-vous préalable avec un Opérateur d'enregistrement.

Les modalités de prise de rendez-vous auprès de la DDE ainsi que les formulaires de demande de Certificats en vigueur sont disponibles depuis la page suivante : https://spe.gouv.mc/entreprises.

Les copies des justificatifs d'identité du Représentant légal et/ou du Mandataire de certification et du Porteur, respectivement du RC, en cours de validité (carte d'identité, passeport ou titre de séjour) seront à fournir à la DDE selon les conditions en vigueur. La personne qui se présentera en présentiel à la DDE pour le processus d'enregistrement devra également présenter l'original de sa pièce d'identité.

Les formulaires contiennent les présentes CGU et les signatures manuscrites des personnes requises. Ils doivent dater de moins de trois (3) mois par rapport à la date de rendez-vous.

Cette demande fait l'objet d'une vérification et d'une validation par l'AE, préalables à la délivrance du Certificat électronique.

La demande est tracée et conservée pendant dix (10) ans après production du ou des certificat(s) attenant(s).

6.2 REMISE DU CERTIFICAT ET ACCEPTATION

Pour les Certificats personnes physiques :

- Délivrance des certificats par l'opérateur d'enregistrement en face à face avec le Porteur.
- Le Porteur est amené à valider le contenu du certificat lors du contrôle qualité réalisé par l'opérateur d'enregistrement. Le certificat fait ainsi l'objet d'une acceptation explicite par le Porteur au moment de sa remise.
- Signature du document de remise des certificats. Ce document est archivé dans le dossier d'enregistrement du Porteur.

Pour les Certificats de cachet :

- Délivrance des certificats par l'opérateur d'enregistrement en face à face avec le RC ou par email en cas de cachet serveur
- Le RC est amené à valider le contenu du cachet lors de sa mise en œuvre.
- Signature du document de remise des certificats. Ce document est archivé dans le dossier d'enregistrement du RC.

A l'issue du processus de remise du Certificat, l'Opérateur d'enregistrement remet au Porteur, respectivement au RC :

- la facture correspondant à la demande ;
- un document indiquant le code d'activation pour chaque Certificat délivré, à charge pour le Porteur, respectivement le RC, dans le mois qui suit cette remise, de se connecter à l'URL qu'il aura reçu en parallèle par mail et de rentrer le code d'activation pour récupérer le code PIN correspondant à son Certificat. A l'issue, il reçoit à nouveau par mail un code de révocation lui permettant, le cas échéant, de révoquer par lui-même son Certificat.

Le service d'émission des certificats qualifiés a été évalué par un organisme accrédité par le Comité Français d'Accréditation (COFRAC). Ce service est conforme à la PC publiée.

6.3 ACTIVATION ET UTILISATION DU CERTIFICAT

Lors de la génération des certificats électroniques sur carte à puce, deux actions se produisent :
• un courrier papier contenant le code d'accès est imprimé et remis au Porteur, respectivement au RC ou au mandataire le cas échéant, par l'opérateur d'enregistrement,

• un e-mail automatique contenant une URL d'activation est envoyé au Porteur, respectivement au RC

Le code d'accès, aussi appelé code d'activation, permet au Porteur, respectivement au RC, de générer son code PIN à 6 chiffres en cliquant sur l'URL indiquée dans l'e-mail qu'il a reçu. Un document PDF contenant le code PIN est alors généré, le Porteur, respectivement le RC, doit le conserver précieusement. (Il n'est pas possible de choisir ni de modifier son code PIN).

Informations importantes sur le code d'activation et le code PIN :
Tant que le Porteur, respectivement le RC, n'a pas activé le lien, l'opérateur d'enregistrement peut renvoyer l'e-mail (uniquement à l'adresse e-mail qui est contenue dans le certificat).
Une fois que le Porteur, respectivement le RC, a saisi le code d'activation après avoir cliqué sur le lien, il accède au lien de téléchargement du PDF contenant son code PIN. Il ne peut cliquer de nouveau sur le lien qui génère le PDF que pendant les 24h suivantes.

Si le Porteur, respectivement le RC, muni de sa carte, saisit un code PIN erroné, son code PIN sera bloqué après 5 tentatives infructueuses. Dans ce cas-là, le Porteur, respectivement le RC, devra réaliser une nouvelle demande de Certificat auprès de l'AC Entreprises.

Un e-mail automatique contenant son code de révocation est envoyé au Porteur, respectivement au RC après la génération du code PIN.

Le Certificat ne sert qu'aux usages définis à l'article 4 des présentes CGU.

6.4 RENOUVELLEMENT DU CERTIFICAT

Le Certificat est valable trois (3) ans.

Le Porteur, respectivement le RC, et le Mandataire de certification sont avertis par l'AE de l'expiration proche de son Certificat par courriel 45, 30 et 15 jours avant l'expiration.

La procédure de traitement d'une demande de nouveau Certificat est la suivante :

- le Porteur ou le Responsable du Certificat reçoit les notifications de l'AE indiquant l'expiration proche des Certificats ;
- le Porteur ou le Responsable du Certificat sollicite un RDV par courriel au esign@gouv.mc pour une remise en face-à-face du nouveau Certificat ;
- lors d'un renouvellement, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

Les éventuelles modifications apportées au corpus documentaire (notamment la PC et les CGU) par rapport à celui ayant prévalu à la délivrance du précédant Certificat sont mises à disposition du Porteur, respectivement du RC, qui en prend connaissance en consultant le site dédié.

Dans tous les cas, les CGU doivent être lues et acceptées.

6.5 REVOCATION DU CERTIFICAT

Les causes possibles d'une révocation sont décrites dans la PC de l'AC Entreprises (consultable à l'adresse suivante : https://spe.gouv.mc/entreprises).

La demande de révocation doit être formulée dès connaissance de l'évènement correspondant.

Le service de révocation des certificats, est disponible en 24/7, 365 jours par an, sauf cas de force majeure qui sera dans ce cas annoncé sur le site mconnect.gouv.mc.

- Révocation d'un certificat avec le code de révocation :

Le processus de révocation en libre-service par le Porteur, respectivement le RC, se fait en ligne de la manière suivante :

- le Porteur, respectivement le RC, se connecte à l'URL de révocation https://fo.certinomis.com/pro, bouton « Révoquer un certificat » ;
- il saisit son code de révocation qui figure dans une notification par courriel reçue après, le cas échéant, activation de son certificat. ;
- il sélectionne le certificat à révoquer, ainsi qu'un motif de révocation ;
- cela déclenche la révocation par l'AC. Le numéro de série du certificat révoqué apparaîtra dans la prochaine LCR (Liste des Certificats Révoqués) publiée ;
- le Porteur, respectivement le RC, reçoit par courriel une notification de la révocation ;
- l'opération est enregistrée dans les journaux d'événements.

Le Porteur, respectivement le RC, peut être, le cas échéant, remplacé par le Mandataire de Certification ou le Représentant Légal dès lors que le code de révocation est connu de manière légitime.

- Révocation d'un certificat en cas de perte du code de révocation :

Le Porteur, respectivement le RC, peut avoir perdu son code de révocation. Le Représentant Légal voire le Mandataire de Certification peuvent vouloir, pour des raisons légitimes, révoquer un certificat (licenciement, départ, départ en retraite, maladie, etc.).

Dans ce cas, le demandeur, qu'il soit le Porteur, le Responsable de Certificat de personne morale, le Représentant Légal ou le Mandataire de Certification, se présente en personne à la DIRECTION DU DÉVELOPPEMENT ÉCONOMIQUE aux heures et jours ouvrés muni d'une pièce d'identité en cours de validité ou contacte le service par téléphone.

L'authentification de la personne par téléphone se fait par le biais des réponses aux 4 questions personnelles (parmi les 9) que le demandeur aura renseignées lors du dépôt de son dossier d'enregistrement. Une fois la révocation effectuée par l'AE, un mail de confirmation est envoyé au porteur et au mandataire le cas échéant.

Les demandes de révocation sont traitées dans les 24h suivant la prise en compte de la demande.

- Révocation d'un certificat par l'AE ou l'Officier de Sécurité de l'ICN :
- L'AE ou l'Officier de Sécurité de l'ICN peuvent procéder à la révocation d'un certificat, notamment en cas de suspicion de compromission ou de compromission avérée de la clé privée dudit certificat, ou en cas d'utilisation frauduleuse ou non-conforme aux présentes CGU. La demande de révocation peut également émaner du Responsable du C2SC.

- Consultation de l'état d'un Certificat :

Le Porteur, respectivement le RC, peut à tout moment vérifier l'état de ses Certificats en consultant les LCR (Liste des Certificats Révoqués) disponibles, ou en interrogeant le service en ligne d'état des certificats (OCSP) qui intègre une réponse « certificat révoqué » après la date de fin de vie du certificat. Les certificats révoqués restent présents dans la LCR même après leur date d'expiration d'origine. En cas de cessation définitive d'activité de l'AC, une dernière LCR sera émise avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s.

7 OBLIGATIONS

Obligations du Porteur, respectivement du RC, et du Mandataire de certification :

Le Porteur, respectivement le RC, a l'obligation de prendre toutes les mesures propres à assurer la sécurité de ses postes informatiques sur lesquels sont utilisés les supports (carte à puce). Lorsque la DDE fournit le support, ce dernier est conforme aux exigences de sécurité figurant aux chapitres afférents de la PC.

Le Porteur, respectivement le RC, s'engage à conserver le support quel qu'il soit et le code PIN associé sous son contrôle exclusif de manière à préserver l'intégrité et la confidentialité de sa clé privée.

En conséquence, le code PIN ne doit jamais être conservé en clair ni se trouver à proximité de la carte à puce.

Le code PIN ne doit jamais être divulgué sous aucun prétexte. Dans le cas du non-respect de cette obligation le Porteur, respectivement le RC, assumerait l'entière responsabilité des conséquences induites sans recours possible contre Direction du Développement Économique.

Dans le cas d'un cachet serveur, le RC s'engage à générer la CSR puis à conserver la clé privée sous son contrôle exclusif de manière à en préserver l'intégrité et la confidentialité.

Le Porteur, respectivement le RC, doit s'assurer d'utiliser une version toujours à jour de son logiciel de lecteur de PDF.

Si une donnée communiquée par le Porteur, le RC ou le Mandataire de certification venait à évoluer (adresse e-mail, etc.), celui-ci doit en informer l'AE sans délai afin de mettre à jour le dossier enregistré.

La connaissance de la compromission avérée ou soupçonnée des données confidentielles, du non-respect des présentes conditions générales, du décès du Porteur, respectivement le RC, ou de la modification des données contenues dans le Certificat, par le Porteur, par le RC ou par la DDE, emporte obligation, à leur charge, de demander dans les meilleurs délais la révocation du Certificat associé.

Le Porteur, respectivement le RC, s'engage à ne plus 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 cause.

Le Porteur, respectivement le RC, ou le Mandataire de certification s'engage à vérifier l'usage indiqué dans le Certificat.

Tout destinataire d'un document signé par un Porteur, respectivement le RC, peut vérifier l'état révoqué ou non d'un Certificat en vérifiant la liste de Certificats révoqués indiquée par le point de distribution présent dans le Certificat. Dans le cas où le Certificat viendrait à être révoqué, il incombe au destinataire du document signé de déterminer s'il est raisonnable d'accorder sa confiance au Certificat. La responsabilité de la DDE ne pourra en aucun cas être engagée en cas de révocation du Certificat.

Obligations de l'AC :

En cas de demande de révocation par le Porteur, respectivement le RC, la DDE révoque le Certificat dans un délai inférieur à vingt-quatre (24) heures à compter d'une sollicitation par le demandeur.

Les conditions de fin de relation avec l'AC ENTREPRISES sont publiées au paragraphe 4.11 de la PC.

8 RESPONSABILITE

Les Certificats ne doivent pas être utilisés de façon abusive ou malveillante.

De manière générale, le Porteur, respectivement le RC, s'engage à utiliser les Certificats :

- Dans le respect des lois et de la règlementation monégasques, ainsi que des droits de tiers ;
- De manière loyale et conformément à leurs usages ;
- Sous sa responsabilité exclusive.

Le Porteur, respectivement le RC, reconnaît et accepte que la responsabilité de la DDE ne peut être engagée au titre de son activité de délivrance de certificats, notamment en cas d'altération, de toute utilisation illicite ou préjudiciable au Porteur, respectivement au RC, ou à un tiers du réseau par un tiers.

Le Porteur, respectivement le RC, assume l'entière responsabilité des conséquences résultant de ses fautes, erreurs ou omissions.

Le Porteur, respectivement le RC, garantit à l'Administration qu'il est propriétaire des documents qu'il signe ou cachète grâce au Service.

L'Administration n'est pas responsable de la légalité et de la conformité des documents signés grâce à son Service.

L'Administration n'est pas responsable si le cachet ou la signature électronique d'un document ne respecte pas les conditions de signature ou de cachet pour ce type de document.

Le Porteur, respectivement le RC, est seul responsable du cycle de vie des documents qu'il signe ou qu'il cachette : de leur établissement jusqu'au terme de la conservation.

Le Porteur du Certificat, respectivement le RC, s'interdit toute utilisation ou tentative d'utilisation du Certificat des fonctionnalités et des usages autorisés des bi-clés à des fins autres que celles prévues par les présentes et par le Certificat lui-même.

9 MODIFICATIONS

Les termes des présentes CGU peuvent être amendés à tout moment, sans préavis, en fonction des modifications opérées par la DDE, de l'évolution de la législation ou de tout autre motif jugé nécessaire. Le Représentant légal, et le cas échéant le Mandataire, le Porteur ou le RC seront notifiés par email ou

SMS, pour toute modification des CGU. A défaut d'une manifestation de leur part dans un délai de 10 jours francs, la nouvelle version sera considérée comme ayant été acceptée. Tout refus de la nouvelle version des CGU entraînera la révocation des certificats déjà délivrés.

10 LIMITES DE GARANTIES ET DE RESPONSABILITES

En aucun cas la DDE n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre les Porteurs, respectivement les RC, desdits Certificats.

La DDE n'assume aucun engagement ni responsabilité quant à la forme, la suffisance, l'exactitude, l'authenticité, ou l'effet juridique des documents remis lors de la demande de Certificat.

La DDE n'assume aucun engagement ni responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, ni quant aux retards, l'altération ou autres erreurs pouvant se produire dans la transmission de toute communication électronique.

La responsabilité de la DDE ne peut être engagée en cas de compromission de la clé privée. La DDE ne se voit pas confier la conservation et/ou la protection de la clé privée du Certificat.

Les parties conviennent expressément, qu'en aucune façon, la responsabilité de la DDE ne pourra être engagée dès lors que le Porteur, respectivement le RC, n'aura pas effectué de demande de révocation de Certificat conformément aux stipulations des présentes.

11 CONSERVATION DES DONNEES

Des données sont conservées lors de la création du dossier d'enregistrement dès la demande de fourniture de Certificat.

Les informations à caractère personnel sont les informations nominatives du Porteur, respectivement du RC, et du Mandataire de certification et du Représentant légal mentionnés au sein du dossier d'enregistrement.

Il s'agit notamment des informations :

Identité / Situation de famille

- Civilité
- Prénom
- Nom

Adresses et coordonnées

- Adresse e-mail professionnelle
- Numéro de téléphone professionnel (Mobile et/ou Fixe)

Formation-Diplômes-Vie professionnelle

- Dénomination sociale (de l'entreprise)
- Numéro de RCI Rôle au sein de ou pour le compte de l'entreprise
- Adresse du siège social

Données d'identification électronique

Données Certificats pour personne physique :

- Cn = Prénom NOM

- SerialNumber (identifiant unique)
- givenName=Prénom
- SurName=NOM
- ou : organization unit : numéro de RCI 0206 suivi du n° de RCI **ou** RC-MC suivi du n° de RCI
- Title : rôle au sein de ou pour le compte de l'entreprise (optionnel)
- (O : Organization) Raison sociale
- C=MC (country)
- Adresse e-mail professionnelle

Données Certificats pour personne morale :

- Cn = FQDN, nom d'application, nom de service, direction, entité, etc.
- SerialNumber (identifiant unique)
- Locality : Monaco (optionnel)
- State : Monaco (optionnel)
- ou : organization unit : 0206 suivi du n° de RCI **ou** RC-MC suivi du n° de RCI
- (O : Organization) Raison sociale
- C=MC (country)

Réponses personnelles pour déblocage code de révocation

4 réponses personnelles sur 9 questions possibles (permettant d'identifier le Porteur, respectivement le RC, le mandataire de certification ou le représentant légal, si celui-ci a oublié son code de révocation).

Ces données sont conservées pendant dix (10) ans. La durée d'archivage est de sept (7) ans après la date d'expiration du Certificat (la durée de vie d'un Certificat étant de trois (3) ans).

Ces données sont conservées dans un espace sécurisé par CERTINOMIS dans le respect du Règlement Général sur la Protection des Données (RGPD). Pour plus d'information, veuillez consulter : https://www.certinomis.fr/mentions-legales.

Un accord a été passé par l'AMSN avec CERTINOMIS pour accéder à ces informations dans le respect du RGPD.

Direction du Développement Économique conserve durant sept (7) ans après la date d'expiration du Certificat les dossiers d'enregistrement dans un espace sécurisé au sein de l'AE.

La conservation est réalisée dans le respect et avec le niveau de protection adapté aux données à caractère personnel dont la gestion fait l'objet du paragraphe 12.

Les logs techniques sont conservés dans un espace sécurisé pour une durée d'un an, puis sont effacés.

12 PROPRIETE INTELLECTUELLE

Les marques et/ou logos dont est titulaire la DDE, apparaissant sur tous supports, sont des marques protégées par les dispositions légales applicables à Monaco.

Toute représentation ou reproduction totale ou partielle sans autorisation expresse et préalable de l'Administration est interdite et constitue une infraction pénalement sanctionnée par les Cours et Tribunaux monégasques.

13 PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conformément aux dispositions de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée, les informations recueillies dans le cadre de la délivrance d'un certificat de cachet ou de signature électronique sont collectées par l'État de Monaco (**Direction du Développement Économique**) qui agit en qualité de responsable du traitement.

Direction du Développement Économique exploite un traitement d'informations nominatives ayant pour finalité la « **Délivrance de certificats de signature et cachet électroniques destinés aux personnes morales** ».

Le traitement s'inscrit dans le cadre des missions de l'Administration. Il est justifié par :

- Le respect d'une obligation légale : Ordonnance Souveraine n° 11.986 portant création de Direction du Développement Économique.
- La réalisation d'un intérêt légitime poursuivi par l'Administration à travers le développement d'outils et procédés numériques afin de proposer des services numériques de confiance bénéficiant d'un haut niveau de sécurité et d'intégrité de la donnée, conformément à la loi n° 1.383 relative à une Principauté Numérique, modifiée, mais également à ses textes d'applications.

Les informations traitées dans le cadre de la fourniture d'un certificat de cachet ou de signature électronique aux entreprises monégasques sont exclusivement destinées à l'Administration et au prestataire de service de confiance fournissant le guichet en ligne. Les données collectées ne font l'objet d'aucune communication à des fins commerciales ou publicitaires.

Ces informations sont conservées uniquement le temps nécessaire à la finalité précitée, et notamment :

- Identité, Réponses personnelles pour déblocage du code de révocation, adresses et coordonnées, Vie professionnelle, tous documents papier fournis par le demandeur : la durée de conservation de ces données est de dix ans (3 ans de durée de vie du certificat + 7 ans de conservation supplémentaire, conformément aux dispositions réglementaires applicables).

- Les données du certificat : ces certificats ont une durée de vie unique de trois ans.

Les informations demandées dans le cadre du formulaire de demande de certificat de signature ou de cachet électronique pour les entreprises monégasques ont un caractère obligatoire. A défaut du renseignement des mentions obligatoires dans le cadre du formulaire de contact, la demande de création de certificat de signature ou de cachet électronique ne pourra être prise en compte.

Dans le respect des dispositions légales en vigueur en matière de protection des Données personnelles, la personne concernée dispose d'un droit d'accès concernant le traitement de ses Données personnelles ; d'un droit d'opposition à leur traitement ainsi que d'un droit de rectification ou de suppression si les informations la concernant se révèlent inexactes, incomplètes, équivoques, périmées.

Pour exercer ses droits ou pour toute question sur le traitement de vos informations nominatives dans le cadre de la demande de création d'un certificat de signature ou de cachet électroniques, la personne concernée peut former une demande :

- En cliquant ici / En se rendant sur le site gouv.mc, Rubrique « Gouvernement et Institutions »/ Département des Finances et de l'Economie > Direction du Développement Économique > Coordonnées.
- A l'adresse postale suivante :

Direction du Développement Économique
9, Rue du Gabian
MC 98000 MONACO

Pour veiller à la confidentialité de la réponse et nous assurer de répondre uniquement à la personne sujet des données, un justificatif d'identité, en noir et blanc, pourra être demandé au requérant.

Si la personne qui a exercé ses droits estime, après avoir contacté l'Administration, que ses droits n'ont pas été respectés, elle peut introduire une réclamation auprès de la Commission de Contrôle des Informations Nominatives : www.ccin.mc.

La solution technique utilisée par Direction du Développement Économique pour la délivrance de certificats aux entreprises a fait l'objet d'une déclaration CCIN et d'une délibération favorable.

14 LOI APPLICABLE, REGLEMENT DES LITIGES

Les parties conviennent de manière expresse que seule la législation et la règlementation monégasques sont applicables.

Elles s'engagent à rechercher un accord amiable en cas de litige. A l'initiative de la partie demanderesse, une réunion sera organisée. Tout accord de règlement du litige devra être consigné par écrit sur un document signé par un représentant accrédité des deux parties.

En cas de litige relatif à l'interprétation, la formation ou l'exécution du Contrat et faute d'être parvenues à un accord amiable, les parties donnent compétence expresse et exclusive aux tribunaux compétents de la Principauté de Monaco.

15 INDEPENDANCE DES PARTIES ET NON-DISCRIMINATION

L'organisation mise en place par l'AC est dédiée à ses activités et garantit l'étanchéité des rôles. Elle permet de préserver l'impartialité des opérations et assure que les activités de confiance fournies sont pratiquées de façon équivalente pour l'ensemble des bénéficiaires ayant accepté les conditions générales d'utilisation du service et respectant les obligations qui leur incombent.

Dans toute la mesure du possible, l'AC met en œuvre des approches appropriées pour rendre son service accessible à toute personne y compris en situation de handicap, en prenant en compte au cas par cas les spécificités de chaque demandeur.

D'une manière générale, les services fournis par l'AC tels que, notamment, la génération de certificats, la gestion des révocations et le statut des certificats sont exercés de façon indépendante et ne sont donc soumis à aucune pression éventuelle.