INFRASTRUCTURE DE CONFIANCE NATIONALE
AC SERVICES ADMINISTRATIFS

CONDITIONS GENERALES D'UTILISATION

État du document - Classification	Référence
En cours - Publique	2.16.492.1.1.1.1.5.3

Version	Date	Description
1.0	4/11/2021	Version applicable
1.1	04/03/2022	Version modifiée
1.3	30/11/2022	Version modifiée

Table des matières

1 OBJET 2
2 DEFINITIONS 2
3 POINT DE CONTACT 3
4 TYPES DE CERTIFICAT ET USAGES 3
5 LIMITE D'USAGE 4
6 CONDITIONS D'OBTENTION ET D'UTILISATION DU CERTIFICAT 4
6.1 Demande de Certificat et Justificatifs à fournir 4
6.2 Remise du certificat et acceptation 5
6.3 Utilisation du Certificat 6
6.4 Renouvellement des certificats 6
6.5 Révocation 7
7 OBLIGATIONS 8
8 RESPONSABILITE 9
9 LIMITES DE GARANTIES ET DE RESPONSABILITES 9
10 CONSERVATION DES DONNEES 10
11 PROPRIETE INTELLECTUELLE 10
12 PROTECTION DES DONNEES A CARACTERE PERSONNEL 10
13 LOI APPLICABLE, REGLEMENT DES LITIGES 11
14 INDEPENDANCE DES PARTIES ET NON-DISCRIMINATION 12

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 des Ressources Humaines et de la Formation de la Fonction Publique (Ci-après désignée « DRHFFP » ou « DRH ») ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les présentes CGU s'appliquent à tout Demandeur, faisant partie des Services de l'Etat, sollicitant les certificats électroniques proposés par la DRH 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 DRH.

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.

- **C2SC** : Comité de Suivi des Services de Confiance.
- **Certificat** : désigne la Clé publique d'un Porteur, respectivement d'un RC, 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 afférentes figurant à l'adresse suivante : https://spp.gouv.mc/services-administratifs applicables à la date de conclusion du contrat.
- **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 (ICN)** : L'ICN est l'ensemble des 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 (Agence Monégasque de Sécurité Numérique) pour le compte du Gouvernement princier. L'AC SERVICES ADMINISTRATIFS est une des autorités rattachées à l'ICN.
- **Mandataire de certification** : désigne la personne physique ayant reçu mandat du Responsable légal pour gérer tout ou partie de la flotte de certificats de la personne morale pendant leur cycle de vie (processus d'enregistrement comprenant le contrôle du dossier et de l'identité du porteur, processus de renouvellement et de révocation, etc.). Le Responsable 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 DRH en charge du traitement des dossiers de demande de certificats.
- **Porteur** : désigne le Porteur de certificat, personne physique identifiée dans le certificat ;
- **Politique de Certification ou PC** : la PC de l'AC Services Administratifs désigne le document établissant les principes qui s'appliquent à l'AC, aux personnes morales, 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://spp.gouv.mc/services-administratifs.
  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 Services Administratifs : 2.16.492.1.1.1.1.5.1
- **Processus d'enregistrement** : désigne le processus d'enregistrement qui consiste à créer et gérer le dossier de demande de certificat.
- **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.
- **Responsable légal** : à définir en prenant en compte le fait que c'est la/les personnes désignées au RCI ayant autorité sur la structure à laquelle elle est/sont rattachée(s).

3 POINT DE CONTACT

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

- Par courrier postal :
  Direction des Ressources Humaines et de la Formation de la Fonction Publique
  3° étage - Stade Louis II - Entrée H
  1 avenue des Castelans
  BP 672
  98014 MONACO CEDEX
- Par e-mail : esign-services-administratifs@gouv.mc

4 TYPES DE CERTIFICAT ET USAGES

Les types de Certificats délivrés sont les suivants :

- Les certificats de signature, délivrés sur carte à puce et permettant la signature électronique d'une personne physique représentant une personne morale (dans ce cas, les acteurs des organismes du secteur public) ;

- 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, délivrés sur carte à puce permettant de s'authentifier notamment, pour les Opérateurs d'enregistrement, sur le portail de gestion des demandes de certificats électroniques.

Les types de Certificats et usages sont décrits dans la PC de l'AC Services Administratifs, consultable à l'adresse suivante : https://spp.gouv.mc/services-administratifs.

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.

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.

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, reconnaît 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 Services Administratifs.

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 SERVICES ADMINISTRATIFS est disponible, sur rendez-vous, pendant les heures d'ouverture de la DIRECTION DES RESSOURCES HUMAINES ET DE LA FORMATION DE LA FONCTION PUBLIQUE.

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

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

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

Les modalités de prise de rendez-vous auprès de la DRHFFP ainsi que les formulaires de demande de Certificats en vigueur sont disponibles en ligne à l'adresse http://intra/ uniquement accessible depuis un ordinateur du Gouvernement Princier connecté au réseau du Gouvernement, ainsi qu'à l'adresse https://spp.gouv.mc/services-administratifs, en libre accès.

D'une manière générale, le Demandeur doit fournir, à l'appui de sa demande, une copie numérique des pièces justificatives suivantes :

- Justificatif d'identité du Responsable légal ;
- 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).

Les originaux du document concernant les attestations relatives au(x) porteur(s)/responsable(s) de certificat et du mandat du mandataire ainsi que de son engagement, le cas échéant, doivent être produits lors du rendez-vous. La personne présente pour la remise, quel que soit son statut (Porteur/Responsable de certificat, Mandataire ou Responsable légal lorsqu'il ne s'agit pas de l'autorité d'un département ministériel) doit de surcroît présenter l'original de sa pièce justificative d'identité à l'Opérateur d'enregistrement.

Dans le cas particulier d'un service exécutif de l'État, le Demandeur n'est pas tenu de fournir le justificatif d'identité du Responsable légal dès lors qu'il s'agit d'une autorité d'un département ministériel et le document « Attestations concernant le Porteur/Responsable de certificat » ne comporte pas la partie « Autorisation du Responsable légal » ; le Référentiel des personnes habilitées à demander et faire usage de certificats électroniques édicté et maintenu à jour par chaque autorité de département indiquant précisément la nature des certificats électroniques autorisés par personne.

Les formulaires de demande 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.

Un Opérateur d'Enregistrement de la DRH vérifie quotidiennement les éventuelles demandes reçues sur l'adresse e-mail esign-services-administratifs@gouv.mc.

Il vérifie la complétude des formulaires joints et la légitimité du Demandeur à effectuer sa demande au regard des différents référentiels auxquels il a accès.

Les formulaires sont remplis directement sur le PDF afin que l'Opérateur d'enregistrement puisse aisément saisir les données dans l'outil du guichet en ligne.

Si un formulaire est incomplet ou absent il retourne la demande de compléments à l'expéditeur (par retour d'e-mail).

Si le formulaire est complet, l'Opérateur d'Enregistrement est alors en mesure de proposer au Demandeur un rendez-vous pour procéder à l'enregistrement.

La demande est tracée et conservée pendant dix (10) ans après la remise du/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 avec 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 le Mandataire de certification, dans le cas d'un cachet sur carte à puce, ou par email en cas de cachet serveur.
- Le RC, respectivement le Mandataire 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.

Lors de la génération des certificats électroniques sur carte à puce, trois actions se produisent :

- un courrier papier contenant le code d'accès est immédiatement imprimé par l'opérateur d'enregistrement,
- un e-mail automatique contenant une URL d'activation est envoyé au Porteur, respectivement au RC,
- un e-mail automatique contenant son code de révocation lui est également envoyé après la génération du code ¨PIN.

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'après-vente 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 Services Administratifs.

6.3 UTILISATION DU CERTIFICAT

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

6.4 RENOUVELLEMENT DES CERTIFICATS

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 suit le même processus que lors de la première demande.

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 et la demande de certificat(s) formelle.

6.5 REVOCATION

Les causes possibles d'une révocation sont décrites dans la PC de l'AC Services Administratifs (consultable à l'adresse suivante : https://spp.gouv.mc/services-adminitratifs).

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 Porteur, respectivement le RC peut avoir perdu son code de révocation. Le Représentant légal voire le Mandataire de Certification peuvent également vouloir, pour des raisons légitimes, révoquer un certificat (licenciement, départ, départ en retraite, maladie, retrait de l'autorisation dans le référentiel des personnes habilitées, etc.).

Dans ce cas, le demandeur, qu'il soit le Porteur, le Responsable de Certificat de personne morale ou le Représentant de l'organisme public se présente en personne à la DIRECTION DES RESSOURCES HUMAINES ET DE LA FORMATION DE LA FONCTION PUBLIQUE 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.

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 d'AC, du Responsable du C2SC, du référent de signature ou d'une autorité judiciaire.

- 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 DRH 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 la DRH.

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 Adobe Acrobat Reader DC.

Si une donnée communiquée par le Porteur, respectivement 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 du RC, ou de la modification des données contenues dans le Certificat, par le Porteur, respectivement le RC, ou par la DRH, 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 un 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 DRH 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 DRH 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 SERVICES ADMINISTRATIFS 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 DRH 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.

Les termes des présentes CGU peuvent également être amendés à tout moment, sans préavis, en fonction des modifications opérées par la DRH, de l'évolution de la législation ou de tout autre motif jugé nécessaire. Il appartient au Porteur, respectivement au RC, de s'informer desdites conditions.

9 LIMITES DE GARANTIES ET DE RESPONSABILITES

En aucun cas la DRH 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 DRH 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 DRH 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 DRH ne peut être engagée en cas de compromission de la clé privée. La DRH 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 DRH 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.

10 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 mentionnées au sein du dossier d'enregistrement.

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.

La DRHFFP conserve durant sept (7) ans les dossiers d'enregistrement au format papier 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.

11 PROPRIETE INTELLECTUELLE

Les marques et/ou logos dont est titulaire la DRH, 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.

12 PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conformément aux dispositions en vigueur en Principauté de Monaco pour la protection des données à caractère personnel, 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 des Ressources Humaines et de la Formation de la Fonction Publique) qui agit en qualité de responsable du traitement pour le traitement « Délivrance de certificats qualifiés de signature et de cachet électroniques aux personnes dûment habilitées des organismes du secteur public ».

Le traitement s'inscrit dans le cadre des missions de l'Administration. Il est justifié par un motif d'intérêt public. La délivrance de certificats qualifiés de signature et cachet électroniques par la DRHFFP aux personnes dûment habilitées des organismes du secteur public, permet à la DRHFFP, d'exercer, de manière pertinente et appropriée, la mission dont la Direction est investie en application de l'Ordonnance Souveraine n° 1.635 du 30 avril 2008 fixant les attributions de la DRHFFP, son Arrêté Ministériel d'application ainsi que de manière générale l'ensemble des dispositions du corpus réglementaire prévu par la Loi n° 1.482 du 17 décembre 2019 pour une Principauté Numérique et les textes encadrant la délivrance des certificats en Principauté.

Les informations traitées dans le cadre de la fourniture d'un certificat de cachet ou de signature électroniques aux organismes du secteur public sont exclusivement destinées au personnel habilité du Gouvernement Princier de Monaco (DRHFFP, DSN et Référent Signature de chaque Service) et ne font l'objet d'aucune communication à des tiers non habilités.

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 papiers 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 organismes du secteur public monégasque 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 électroniques ne pourra être prise en compte.

Dans le respect des dispositions légales en vigueur en matière de protection des Données personnelles en Principauté de Monaco, la personne concernée dispose d'un droit d'accès concernant le traitement de ses Données personnelles 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 ses 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 » > Ministère d'Etat > Secrétariat Général du Gouvernement > Direction des Ressources Humaines et de la Formation de la Fonction Publique > Coordonnées.
- A l'adresse postale suivante :

Direction des Ressources Humaines et de la Formation de la Fonction Publique

3° étage - Stade Louis II - Entrée H

1 avenue des Castelans

BP 672

98014 MONACO CEDEX

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 la Direction des Ressources Humaines et de la Formation de la Fonction Publique pour la délivrance de certificats aux personnes dûment habilitées des organismes du secteur public a fait l'objet d'une déclaration CCIN et d'une délibération favorable.

13 LOI APPLICABLE, REGLEMENT DES LITIGES

Les parties conviennent de manière expresse que seule la législation et la règlementation monégasque 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.

14 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.