INFRASTRUCTURE DE CONFIANCE NATIONALE
AC GOUVERNEMENT PRINCIER

CONDITIONS GENERALES D'UTILISATION

État du document - Classification	Référence
En cours - Publique	2.16.492.1.1.1.1.3.3

Version	Date	Description
1.1	22/07/2021	Version initiale publiée
2.0	4/11/2021	Version publiée
2.1	08/12/2021	Version publiée
2.3	04/03/2022	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 et d'authentification délivrés par le Gouvernement Princier (Ci-après désignée « Gouvernement ») ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les présentes CGU s'appliquent à tout Porteur (Résident) sollicitant les certificats électroniques proposés par le Gouvernement et utilisant lesdits certificats.

Le Porteur (Résident) 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 :

- **Agent (ou opérateur d'enregistrement)** : désigne l'opérateur de la DSP en charge du traitement des dossiers de demande de génération et de révocation des certificats ;
- **Autorité de Certification ou AC** : désigne l'ensemble des systèmes informatiques qui permettent de créer et révoquer des certificats électroniques. Elle est sous la responsabilité de la Direction de la Sûreté Publique (DSP) ;
- **Autorité d'Enregistrement ou AE** : désigne l'autorité mise en œuvre par la Direction de la Sûreté Publique (DSP), qui assure les fonctions suivantes :
    - Réception des dossiers de demande de certificats ;
    - Réception des dossiers de demande de révocation de certificats ;
    - Vérification de l'identité et de l'habilitation du futur porteur de certificats ;
    - Remise au futur porteur du support cryptographique des certificats nécessaires pour leur utilisation ;
    - 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, 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** : désigne l'ensemble contractuel constitué des présentes CGU, du dossier de demande de certificat ainsi que de la Politique de Certification figurants à l'adresse suivante : https://mconnect.gouv.mc/gouvernement-princier et applicables à la date de conclusion du contrat ;
- **C2SC (Comité de Suivi des Services de Confiance) :** Ce comité est le garant de l'application de la Politique de Certification et de la bonne concordance avec les autres référentiels documentaires.
- **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.

- **Demandeur :** Le demandeur est la personne physique qui effectue une demande auprès de l'Autorité d'Enregistrement pour obtenir une carte de séjour et ainsi un certificat électronique de personne physique.
- **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 GOUVERNEMENT PRINCIER est l'une des autorités rattachées à l'ICN.
- **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.
- **Politique de Certification ou PC** : désigne la PC de l'AC Gouvernement Princier, document établissant les principes qui s'appliquent à l'AC, et à l'ensemble des acteurs intervenant dans le cycle de vie d'un certificat, (consultable à l'adresse suivante : https://mconnect.gouv.mc/gouvernement-princier)
  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 Gouvernement Princier : 2.16.492.1.1.1.1.3.1.
- **Porteur :** désigne le titulaire de la Carte de Séjour et l'usager des Certificats électroniques. C'est la personne physique identifiée dans le Certificat.
- **Processus d'enregistrement** : désigne le processus qui consiste à créer et gérer le dossier de demande de certificat ;

3 POINT DE CONTACT

Les demandes d'informations relatives à la délivrance des cartes de séjour et Certificats électroniques délivrés par la Direction de la Sûreté Publique peuvent être réalisées :

- Par courrier postal : DIRECTION DE LA SÛRETÉ PUBLIQUE - DIVISION DE POLICE ADMINISTRATIVE, Stade louis II, entrée B, étage 1, MC 98000 MONACO
- Par e-mail en remplissant le formulaire suivant : https://service-public-particuliers.gouv.mc/Contactez-l-administration/(entite)/5348/(name)/5729

4 USAGES DES CERTIFICATS

Les types de Certificat délivrés permettent :

- l'authentification d'un Porteur personne physique sur les services en ligne publics et privés partenaires en utilisant sa **carte de séjour** ;
- la signature électronique d'un Porteur personne physique pour signer des documents électroniquement en utilisant sa **carte de séjour** ;
- l'authentification d'un Porteur personne physique sur des services en ligne publics et privés partenaires en utilisant son **smartphone** ;

- la signature électronique d'un Porteur personne physique permettant pour signer des documents électroniquement en utilisant son **smartphone.**

Les types de Certificats et usages sont décrits dans la PC de l'AC Gouvernement Princier (consultable à l'adresse suivante : https://mconnect.gouv.mc/gouvernement-princier).

5 LIMITE D'USAGE

Les Porteurs 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 et du Certificat associé est strictement limitée au service défini par l'identifiant de sa PC.

Le Porteur 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 Gouvernement Princier consultable à l'adresse suivante : https://mconnect.gouv.mc/gouvernement-princier).

6 CONDITIONS D'OBTENTION ET D'UTILISATION DU 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.

6.1 DEMANDE DE CERTIFICAT ET JUSTIFICATIFS A FOURNIR

La prise de rendez-vous pour l'enregistrement du dossier de demande de carte de séjour et de certificats électronique d'authentification et de signature doit être faite auprès de l'AE Direction de la Sûreté Publique (et plus précisément auprès de la Section des Résidents).

Cette sollicitation de la DSP peut être réalisée en ligne par le biais d'un téléservice ou sur place auprès de la Section des Résidents de la DSP.

Les principes et conditions ainsi que les pièces à fournir sont détaillés sur le site du service public particuliers : https://service-public-particuliers.gouv.mc/Nationalite-et-residence/Residence

Le service d'enregistrement des demandes de certificat est disponible pendant les heures d'ouverture de la Section des Résidents.

6.1.1 *Enregistrement de la demande de carte de séjour et de la demande de certificat électronique*

Le texte de référence mentionné ci-dessous définit les contenus visuels et électroniques de la carte de séjour monégasque.

Arrêté Ministériel n° 2021-430 du 17 juin 2021 portant application de l'article 4 de l'Ordonnance n° 3.153 du 19 mars 1964 sur les conditions d'entrée et de séjour des étrangers dans la Principauté, modifiée (Cf Articles 2, 3, 4, 6, 7 et 10)

La demande de carte de séjour vaut demande de certificats électroniques (d'authentification et de signature).

Cette délivrance comprend la prise en charge et l'orchestration de toutes les phases nécessaires à la production d'un titre finalisé, depuis l'enregistrement de la demande du titre jusqu'à sa remise au Porteur. Les étapes sont les suivantes :

- Accueil du demandeur en présentiel à la DSP
- Vérification de l'identité du demandeur
- Prise de la biographie
- Prise de la biométrie (prise de la photo ainsi que des empreintes)
- Complétion du formulaire de demande de certificat électronique lié à l'identité numérique correspondant au reçu d'enrôlement

La demande de certificats électroniques d'authentification et de signature se matérialise par le reçu d'enrôlement. Ce document est automatiquement généré par le système lors du rendez-vous de demande en face à face entre l'opérateur d'enregistrement et le porteur.

Le document de demande récapitule les champs et données relatifs au porteur, il est daté et signé par l'opérateur ainsi que par le porteur et conservé par les deux parties par la suite.

- Acceptation des CGUs (via la signature du reçu d'enrôlement)
- Instruction du dossier :
    - Vérification de la complétude du dossier de demande
    - Vérification de l'identité et de la légitimité du demandeur

6.1.2 *Traitement de la demande*

- Validation de la demande par l'Opérateur d'Enregistrement (agent DSP)
- Validation du dossier complet par le Directeur de la Sûreté Publique
- Génération des certificats électroniques :
    - Personnalisation électrique de la carte : génération des certificats liés à l'identité numérique
    - Personnalisation graphique de la carte
- Contrôle qualité de la carte et des certificats électroniques par l'opérateur d'enregistrement : vérification des données biographiques et biométries, de la MRZ et des certificats électroniques ainsi que du conteneur ICAO

6.2 REMISE DU CERTIFICAT ET ACCEPTATION

6.2.1 *Déroulé du processus de remise des Certificats électroniques embarqués dans la carte de séjour*

- Accueil du Demandeur en présentiel à la DSP
- Vérification de la biométrie (empreintes et identité du porteur)

- Acceptation tacite du certificat par le Porteur (validation par le Porteur des certificats électroniques) *
- Délivrance de la carte de séjour et des certificats en face à face
- Délivrance d'un bordereau de remise contenant un récapitulatif des éléments liés à la délivrance des certificats ainsi que le code de révocation à destination du Porteur

*Le Porteur dispose de 7 jours francs à compter de la remise de la carte de séjour pour vérifier l'exactitude du contenu des certificats qui lui ont été délivrés (voir mconnect.gouv.mc/logiciel), qu'il ait activé ou non les moyens d'utilisation de son identité numérique par génération du code PIN.

En cas d'erreur sur son identité dans les certificats, le Porteur prend contact avec la Section des Résidents afin de demander la délivrance d'une nouvelle carte de séjour et de nouveaux certificats.

6.2.2 *Déroulé du processus d'activation des moyens d'utilisation de l'identité numérique du porteur*

Le Porteur peut activer les moyens d'utilisation de son identité numérique lors de la remise de la carte de séjour auprès de l'opérateur de la Section des Résidents, ou ultérieurement sur la borne interactive disponible en libre-service à la Section des Résidents de la Direction de la Sûreté Publique.

Le Porteur peut décider d'activer ou non les moyens d'utilisation de son identité numérique.

Les étapes d'activation des moyens liés à l'identité numérique (génération du code PIN) auprès de l'opérateur sont les suivantes (après processus de remise) :

- Mise à disposition du Porteur d'un Pinpad (périphérique de saisie)
- Saisie du code PIN* choisi par le Porteur (le PIN saisi reste confidentiel, il n'est affiché ni au Porteur ni à l'opérateur.)
- Confirmation du choix par une deuxième saisie du code PIN
- Validation par l'opérateur de l'activation des moyens d'utilisation de l'identité numérique sur le système (lorsque les deux PINs correspondent bien)

Les étapes d'activation des moyens liés à l'identité numérique (génération du code PIN) sur la borne interactive en libre-service sont les suivantes :

- Lecture de la carte de séjour grâce au lecteur de la borne interactive
- Sélection de l'option « Activer mon identité numérique » sur l'écran
- Vérification biométrique de l'identité du porteur-par reconnaissance faciale (comparaison de la photo contenue dans la puce ICAO avec le visage du porteur)
- Saisie du code PIN* choisi par le porteur (le PIN saisi reste confidentiel, il n'est pas affiché à l'écran en clair.)
- Confirmation du choix par une deuxième saisie du code PIN
- Validation automatique par la borne interactive de l'activation des moyens d'utilisation de l'identité numérique sur le système (lorsque les deux PINs correspondent bien)

**Le code PIN ne doit pas avoir :*

- *5 fois le même digit*
- *5 digits qui se suivent*
- *5 digits qui correspondent aux 5 derniers digits du numéro de document, dans le même ordre*

6.3 UTILISATION DES CERTIFICATS

Toute carte de séjour contient une puce cryptographique.

La puce contient deux types de Certificats :

- Un Certificat d'authentification ;
- Un Certificat de signature électronique.

Les deux certificats sont composés des mêmes champs :

- Noms et prénoms du porteur ;
- Pays d'émission ;
- Numéro de série du Certificat ;
- Autorité de Certification ;
- La date de début de validité ;
- La date de fin de validité.

Les Certificats électroniques permettant au Porteur de s'authentifier ou de signer via son smartphone sont dérivés des Certificats électroniques de la carte de séjour.

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

Le service d'authentification sur ***M* CONNECT** est disponible en 24/7, 365 jours par an, sauf cas de force majeure annoncé, dans ce cas, à travers ce portail.

Par ailleurs, des notifications sont réalisées sur le site de référence mconnect.gouv.mc en cas de problèmes susceptibles de porter atteinte à l'intégrité du service.

6.4 RENOUVELLEMENT DES CERTIFICATS

Les Certificats électroniques ont une durée de vie maximale de trois (3) ans.

Les cartes de séjour délivrées par la Direction de la Sûreté Publique peuvent avoir des durées de validité différentes selon la catégorie de la carte de séjour délivrée :

- La catégorie « temporaire » est valable 1 an ;
- La catégorie « ordinaire » est valable 3 ans ;
- La catégorie « conjoint de monégasque » est valable 5 ans ;
- La catégorie « privilégié » est valable 10 ans.

Dans le cas des catégories « temporaire » et « ordinaire », le renouvellement pourra s'effectuer avec la demande et la délivrance d'une nouvelle carte de séjour et un nouveau certificat.

Pour les catégories de cartes de séjour dont la durée de validité est strictement supérieure à 3 ans (« privilégiée » et « conjoint »), le porteur devra réaliser le renouvellement des certificats électroniques en libre-service sur la borne interactive à disposition à la Section des Résidents de la DSP.

Le porteur s'authentifie sur la borne interactive en saisissant son code PIN et procède au renouvellement directement sur la borne. Le renouvellement dure environ 3 minutes et est immédiatement effectif, permettant l'usage des certificats électroniques sans l'édition d'un nouveau titre.

6.5 REVOCATION

Les causes possibles d'une révocation sont décrites dans la PC de l'AC Gouvernement Princier (consultable à l'adresse suivante : https://mconnect.gouv.mc/gouvernement-princier)

Le service de révocation des certificats est disponible en 24/7, 365 jours par an, sauf cas de force majeure annoncée, dans ce cas, à travers le portail ***M* CONNECT**.

Les Certificats peuvent notamment être révoqués pour les raisons suivantes :

- **Expiration du Certificat** : les certificats électroniques ont une durée de vie de 3 ans, ensuite, ils sont automatiquement révoqués ;

- **Demande de révocation de la part du Porteur ou de son Représentant légal** (perte ou vol de la carte ou compromission des Certificats) ;

En cas de perte ou de vol de la carte et de possible compromission de ses Certificats, le Porteur doit utiliser le code de révocation transmis le jour de la délivrance du titre (inscrit sur le bordereau de remise) pour compléter le formulaire de révocation disponible en ligne via ce lien : https://mconnect.gouv.mc/formulaire-de-demande-de-revocation-des-certificats-electroniques-pour-les-titulaires-de-carte-de-sejour. Il sera notifié par l'AE de la révocation effective de ses certificats.

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

En cas de perte du code de révocation, le Porteur doit se présenter en personne à la Direction de la Sûreté Publique (Section des Résidents) afin de demander la révocation des Certificats.

- **Délivrance d'un nouveau titre, remplaçant le précédent** et entraînant la révocation des Certificats électroniques du précédent titre (ex : renouvellement, duplicata…)

- **Départ du Porteur de la Principauté**, entraînant une action de l'Agent de la DSP sur l'application métier dédiée et invalidant les Certificats électroniques. Si le Porteur a quitté la Principauté ou n'est plus Résident, alors son Certificat est invalidé et son identité numérique n'est plus valable.

En cas de départ de la Principauté, les démarches en ligne en cours réalisées via l'utilisation de ses Certificats électroniques ne pourront aboutir étant donné que ces Certificats auront été révoqués. De fait, il est recommandé au Porteur de récupérer sur les services en ligne concernés les données et documents qu'il souhaitera conserver et le concernant avant de notifier son départ de la Principauté.

- **Décès du Porteur**, entraînant une action de l'Agent de la DSP sur l'application métier dédiée et invalidant les Certificats électroniques.

- **Utilisation frauduleuse ou non-conforme aux présentes CGU :** entrainant la révocation des Certificats de la part de l'AC ou de l'Officier de Sécurité de l'ICN conformément à l'article 5 ci-avant. Cette demande de révocation peut être sollicitée par le Responsable du C2SC.

Processus de remise du code de révocation au Porteur :

Lors de la remise de la carte de séjour, tout Porteur (Résident) reçoit un bordereau de remise.

Le bordereau de remise contient notamment le code de révocation (de type 123456).

Le code de révocation correspond au numéro de demande de la carte.

L'agent explique au Porteur que ce bordereau doit être conservé précieusement, et que le code de révocation lui sera indispensable pour révoquer à distance ses certificats électroniques.

Consultation de l'état d'un Certificat :

Le Porteur 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

Le porteur 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).

Le porteur a l'obligation d'installer le logiciel Smart Card Manager (disponible via ce lien : https://mconnect.gouv.mc/logiciel) afin de pouvoir utiliser les Certificats électroniques.

L'Administration n'est nullement responsable de l'utilisation de ce logiciel.

Le Porteur s'engage à conserver le support et le code PIN associé sous son contrôle exclusif de manière à en 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 assumerait l'entière responsabilité des conséquences induites sans recours possible contre la Direction de la Sûreté de Publique et le Gouvernement Princier de Monaco.

Lorsque la DSP délivre le titre, ce dernier est conforme aux exigences de sécurité figurant aux chapitres afférents de la PC.

Dans le cas de l'usage du Certificat électronique de signature, le Porteur doit s'assurer d'utiliser une version toujours à jour de son logiciel Adobe Acrobat Reader DC et d'en respecter les conditions générales d'utilisation.

Si une donnée communiquée par le Porteur venait à évoluer, celui-ci doit en informer la DSP sans délai afin de mettre à jour le dossier enregistré et délivrer une nouvelle carte de séjour selon les cas.

La connaissance de la compromission avérée ou soupçonnée des données confidentielles, du non-respect des présentes conditions générales ou de la modification des données contenues dans le Certificat, par le porteur ou par la DSP, emporte obligation, à leur charge, de demander dans les meilleurs délais, la révocation du Certificat associé, au risque de s'exposer à une usurpation d'identité.

Le Porteur 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 s'engage à vérifier l'usage indiqué dans le Certificat.

Tout destinataire d'un document signé par un Porteur 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 DSP 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, la DSP révoque le Certificat dans un délai inférieur à vingt-quatre (24) heures à compter d'une sollicitation par le Porteur.

Les conditions de fin de relation avec l'AC GOUVERNEMENT PRINCIER 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 s'engage à utiliser les Certificats :

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

Le Porteur reconnaît et accepte que la responsabilité de la DSP 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 ou à un tiers du réseau par un tiers.

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

Le Porteur garantit à l'Administration qu'il est propriétaire des documents qu'il signe grâce à son Certificat électronique de signature.

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

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

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

Le Porteur 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 DSP, de l'évolution de la législation ou de tout autre motif jugé nécessaire. Il appartient au Porteur de s'informer desdites conditions.

La version des CGUs qui fait foi est celle disponible sur le site de publication. https://mconnect.gouv.mc/gouvernement-princier

9 LIMITES DE GARANTIES ET DE RESPONSABILITES

En aucun cas la DSP n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre les utilisateurs des certificats et/ou les Porteurs.

La DSP 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 DSP 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 DSP ne peut être engagée en cas de compromission de la clé privée. La DSP 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 DSP ne pourra être engagée dès lors que le Porteur 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 carte de séjour et par conséquent de fourniture de Certificat.

Les informations à caractère personnel sont les informations nominatives du Porteur mentionnées au sein du dossier d'enregistrement.

Il s'agit notamment des informations :

Etat civil

- Nom
- Prénoms
- Nom d'usage
- Date et heure de naissance
- Lieu de naissance
- Sexe à la naissance
- Initiales (ex : JEAN DUPOND, JD)

Adresses et coordonnées

- Adresse postale

Données d'identification électronique

- Données du conteneur ICAO : ZLA (MRZ)

Données des Certificats électroniques d'authentification et de signature

- Noms et prénoms du porteur
- Pays d'émission
- Le numéro de série du Certificat
- L'Autorité de Certification
- La date de début de validité
- La date de fin de validité

Données biométriques

- Photo
- Empreintes

Signature

- Signature manuscrite (réalisée sur un pad)

Données propres à la demande et à la carte

- Numéro de demande
- Numéro de carte
- Date de début/fin de validité
- Autorité de délivrance
- CAN (card access number pour récupérer le PUK))

Les dossiers de demandes des titres régaliens sont conservés indéfiniment à titre d'archives historiques.

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

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.

11 PROPRIETE INTELLECTUELLE

Les marques et/ou logos dont est titulaire la DSP, 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

Dans le cadre de la création d'une identité numérique à Monaco, l'Etat de Monaco/Direction de la Sûreté Publique met en œuvre un traitement de données personnelles ayant pour finalité « Gestion d'une plateforme permettant la délivrance et la gestion des cartes de séjour ».

Les données personnelles collectées dans le cadre du traitement sont collectées de manière indirecte et ont pour origine la personne concernée (pour la photo et les empreintes) ou le fichier source constituant la base de données relatives aux résidents en Principauté.

Les seuls destinataires des données sont le personnel strictement habilité de la Direction de la Sûreté Publique.

Conformément aux dispositions applicables en matière de protection des données personnelles en Principauté de Monaco, les personnes concernées par le traitement disposent d'un droit d'accès aux données personnelles les concernant, ainsi que le droit de demander à ce que soient rectifiées, mises à jour ou supprimées les données inexactes, incomplètes ou périmées. Pour exercer ses droits les personnes peuvent former une demande écrite, en précisant l'objet de la demande, ainsi que son nom, prénom et date de naissance par voie postale, à l'adresse suivante :

Direction de la Sûreté Publique

Stade louis II, entrée B, étage 1

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.

La solution technique utilisée par la DSP pour la délivrance de certificats électroniques a fait l'objet de délibérations favorables de la part de la CCIN :

- Délibération n° 2021-109 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la modification du traitement automatisé d'informations nominatives ayant pour finalité « Gestion d'une plateforme permettant la délivrance et la gestion des cartes de séjour » exploité par la Direction de la Sûreté Publique présenté par le Ministre d'État.
- Délibération n° 2021-110 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Gestion des identités numériques au travers du Registre National Monégasque de l'Identité Numérique » dénommé « RNMIN » exploité par la Direction des Services Numériques présenté par le Ministre d'État.
- Délibération n° 2021-111 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Gestion des moyens d'utilisation de l'identité numérique inscrits sur les cartes d'identité monégasque et les cartes de séjour (certificats, code CAN et PUK) » dénommé « CLCM » exploité par la Direction des Services Numériques et présenté par le Ministre d'État.
- Délibération n° 2021-112 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Fourniture

des services de confiance pour l'identité numérique » dénommé « MConnect et MConnect Mobile » exploité par la Direction des Services Numériques et présenté par le Ministre d'État.

- Délibération n° 2021-113 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Plateforme d'activation et de gestion de l'identité numérique après délivrance du titre » dénommé « kiosque » exploité par la Direction des Services Numériques présenté par le Ministre d'État.
- Délibération n° 2021-142 du 23 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Réaliser une signature entre plusieurs parties par le biais d'une démarche en ligne » exploité par la Direction des Services Numériques présenté par le Ministre d'État.
- Délibération n° 2021-141 du 23 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Réaliser une déclaration sur l'honneur par le biais d'une démarche en ligne » exploité par la Direction des Services Numériques présenté par le Ministre d'État.
- Délibération n° 2021-140 du 23 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Permettre l'utilisation de l'identité numérique des monégasques et résidents par le biais d'une application mobile dédiée » dénommé « MConnect Mobile » exploité par la Direction des Services Numériques présenté par le Ministre d'État.

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.