INFRASTRUCTURE DE CONFIANCE NATIONALE
AC SERVICES NUMERIQUES
CONDITIONS GENERALES D'UTILISATION

État du document - Classification	Référence
En cours - Publique	

Version	Date	Description
1.0	11/11/2024	Version intiale publiée

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 la Direction des Services Numériques (ci-après désignée « DSN ») 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 DSN et utilisant lesdits certificats.

Le Porteur 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 DSN 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.

Autorité d'Enregistrement ou AE : désigne l'Autorité mise en œuvre par la Direction des Services Numériques (DSN), qui assure les fonctions suivantes :

Réception des dossiers de demande de génération des certificats ;

Réception des dossiers de demande de révocation des certificats ;

Vérification de l'identité et de l'habilitation du Demandeur de certificats ;

Remise au futur porteur, des certificats ;

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** : 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://mconnect.gouv.mc/services-numeriques 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.
- **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 SERVICES NUMERIQUES est 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.
- **Opérateur d'enregistrement** : désigne l'opérateur de la DSN en charge du traitement des dossiers de demande de certificats.
- **Politique de Certification ou PC** : la PC de l'AC SERVICES NUMERIQUES désigne le document établissant les principes qui s'appliquent à l'AC, aux Porteurs, respectivement aux RC, intervenant dans l'ensemble du cycle de vie d'un certificat, (consultable à l'adresse suivante : https://mconnect.gouv.mc/services-numeriques)
  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 Numériques : *Numéro d'OID à venir.*
- **PVID** : **(Prestataire de Vérification d'Identité à Distance) :** Solution permettant la vérification de l'identité du Demandeur de Certificats à Distance. Le PVID utilisé par le Téléservice MConnect est qualifié par l'AMSN (cf AM n° 2024-164).
- **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.

3 POINT DE CONTACT

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

- Par courrier postal : Direction des Services Numériques - 2 rue du Gabian - Immeuble "Les Industries" - BP 673 MC 98014 Monaco Cedex
- Par e-mail : identitenumerique@gouv.mc.

4 TYPES DE CERTIFICATS ET USAGES

Les types de Certificats délivrés sont les suivants :

- Le Certificat de signature électronique d'un Porteur personne physique pour signer des documents électroniquement sur des services en ligne publics et privés partenaires en utilisant son smartphone ;
- Le Certificat d'authentification d'un Porteur personne physique sur des services en ligne publics et privés partenaires en utilisant son smartphone ;
-

Les types de Certificats et usages sont décrits dans la PC de l'AC Services Numériques (consultable à l'adresse suivante : https://mconnect.gouv.mc/services-numeriques).

Des notifications sont réalisées sur le site de référence https://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 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 Services Numériques consultable à l'adresse suivante : https://mconnect.gouv.mc/services-numeriques.

6 CONDITIONS D'OBTENTION ET D'UTILISATION DU CERTIFICAT

6.1 DEMANDE DE CERTIFICAT ET JUSTIFICATIFS A FOURNIR

La demande de création d'une identité numérique monégasque et de délivrance de certificats électroniques associés est soumis à une invitation préalable d'un Service de l'Etat.

La loi identité numérique (2019-1483) définit le cadre de délivrance d'une identité numérique monégasque.

Le service d'enregistrement proposé par l'AC SERVICES NUMERIQUES est disponible en 24/7, via une URL communiquée au Demandeur par un Service de l'Etat du Gouvernement Princier.

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,
- lors d'un rendez-vous 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 MConnect de demande de création d'une identité numérique monégasque et de délivrance des certificats électroniques associés, disponible via l'URL communiquée par un Service de l'Etat

Pour ce faire, l'usager doit avoir :

- Un titre d'identité supporté par le PVID (liste des documents supportés disponible ici)
- Un téléphone mobile muni d'une caméra
- Une connexion internet
- Un accès à sa boite email

Le Demandeur atteste avoir pris connaissance et accepter les présentes CGU, et formalise sa demande de certificats électroniques.

Il renseigne les informations suivantes dans le formulaire en ligne :

- Adresse email
- Numéro de téléphone
- Nom de naissance
- Prénom(s)

Le Demandeur est ensuite redirigé vers le processus de vérification d'identité à distance, opérée par le Prestataire de Vérification d'Identité à Distance qualifié par l'Agence Monégasque de Sécurité Numérique.

Une fois finalisé ce parcours, la vérification de l'identité du demandeur tarde environ 15 minutes.

Pendant ce labs de temps, l'usager est invité à installer l'application MConnect Mobile sur son téléphone mobile. Cette application lui permettra de faire usage de ses certificats électroniques. L'application MConnect Mobile est disponible pour IOS sur l'Apple Store, et pour Android sur Google Play.

Lorsque le processus de vérification d'identité à distance est clos, le Demandeur en est notifié par SMS, et est invité à consulter l'état de sa demande dans son interface du téléservice.

Si l'identité du Demandeur a été validée, les données d'identité fournies par le PVID, telles que renseignées sur le titre d'identité présenté par le Demandeur, lui sont affichées. Ce dernier est invité à confirmer leur exactitude, ou à contacter le support usager dans le cas d'une erreur.

Une fois validées par le Demandeur, ces données seront utilisées pour créer son identité numérique le cas échant, ainsi que les certificats d'authentification et de signature électroniques associés.

Le Demandeur est alors redirigé vers l'application MConnect Mobile via un lien contextualisé lui permettant de finaliser le processus de délivrance de ses certificats électroniques.

La demande est tracée et conservée pendant sept (7) ans après production du ou des certificat(s) attenant(s).

Si l'identité du Demandeur n'a pas pu être validée, ce dernier est invité à refaire le processus de vérification d'identité à distance, ou à contacter un opérateur de l'AE DSN afin de réaliser sa demande lors d'un rendez-vous présentiel avec un Opérateur (voir chapitre 6.1.2).

6.1.2 Lors d'un rendez-vous auprès d'un Opérateur d'Enregistrement

En cas de problème lors de la demande par le Téléservice, le Demandeur peut réaliser sa demande de certificats électroniques auprès d'un Opérateur d'Enregistrement.

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

Les modalités de prise de rendez-vous auprès d'un Opérateur d'Enregistrement de l'AE DSN sont disponibles depuis la page suivante : https://mconnect.gouv.mc/contact-aedsn.

Le Demandeur devra se présenter lors du rendez-vous avec l'Opérateur d'Enregistrement avec :

- Un titre d'identité en cours de validité
- Un téléphone mobile de type smartphone avec une connexion internet
- Un accès a sa boîte email

L'Opérateur d'Enregistrement fournira un formulaire de demande papier au Demandeur, par lequel le Demandeur attestera avoir pris connaissance et accepter les présentes Conditions Générales d'Utilisation.
Le formulaire de demande contient les présentes CGU et la signature manuscrite du Demandeur.

La demande fait l'objet d'une vérification et d'une validation par l'AE, préalables à la délivrance des Certificats électroniques.

La demande est tracée et conservée pendant sept (7) ans après production du ou des certificat(s) attenant(s).

6.2 REMISE DU CERTIFICAT ET ACCEPTATION

La remise des certificats s'effectue lors de l'installation par l'usager de son identité numérique dans l'application MConnect Mobile.

Les deux certificats électroniques, d'authentification et de signature électronique, sont alors délivrés.

Le Porteur dispose de 10 jours francs à compter de la remise de ses certificats via l'Application MConnect Mobile pour vérifier l'exactitude du contenu des certificats qui lui ont été délivrés.

Il peut pour cela consulter les données affichées dans son Application MConnect Mobile, ou lors de la création de via son Profil MConnect (https://profil.mconnect.mc).

Pour finaliser la procédure, l'usager doit compléter son Profil MConnect (https://profil.mconnect.mc). Il sera ainsi en capacité de renouveler et révoquer ses certificats électroniques en toute autonomie, et il sera informé en amont de l'expiration de ses certificats afin d'anticiper leur renouvellement.

6.3 ACTIVATION ET UTILISATION DU CERTIFICAT

Lors de l'installation de l'identité numérique dans l'Application MConnect Mobile du Porteur, les certificats d'authentification et de signature électronique sont délivrés.
Le Porteur est invité à choisir un code à 6 chiffres pour déverrouiller l'accès à l'Application MConnect Mobile. C'est ce code qui permet de faire usage desdits certificats.
Le Porteur peut à tout moment modifier ce code à partir de l'onglet « Réglages » de l'Application MConnect Mobile.
En cas d'oubli du code, le Porteur devra réaliser une demande de renouvellement de ses Certificats auprès de l'AE DSN.

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.

S'il a créé son Profil MConnect, le Porteur est averti de l'expiration prochaine de ses Certificats par courriel et/ou SMS 6 mois, 3 mois, 1 mois, 15 et 5 jours avant l'expiration.

La procédure de traitement d'une demande de nouveaux Certificats est la suivante :

Si le Porteur a créé son Profil MConnect, il peut réaliser sa demande de renouvellement en toute autonomie, en 24/7, depuis l'url https://profil.mconnect.mc :

Soit en s'authentifiant via MConnect et son application MConnect Mobile, si ses certificats n'ont pas encore expiré ;

Soit en procédant à un Parcours de Vérification d'Identité à Distance, si ses certificats ont expiré, ou s'il souhaite changer de téléphone mobile. La procédure d'identification et de validation de la demande de renouvellement est alors identique à la procédure d'enregistrement initial, mais se fait depuis l'url https://profil.mconnect.mc.

Si le Porteur n'a pas créé son Profil MConnect, ou s'il rencontre un problème lors du traitement de sa demande via le Téléservice Profil MConnect, il sollicite un RDV auprès d'un Opérateur d'Enregistrement de l'AE DSN. Les modalités de prise de rendez-vous auprès d'un Opérateur d'Enregistrement de l'AE DSN sont disponibles depuis la page suivante : https://mconnect.gouv.mc/contact-aedsn. La procédure d'identification et de validation de la demande de renouvellement est alors 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 des précédents Certificats sont mises à disposition du Porteur 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 Services Numériques (consultable à l'adresse suivante : https://mconnect.gouv.mc/services-numeriques).

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 https://mconnect.gouv.mc.

Révocation d'un certificat par le Porteur, en toute autonomie :

Pour procéder à la révocation de ses certificats en toute autonomie, l'usager doit :

- Soit avoir accès à son Application MConnect Mobile avec son identité numérique
- Soit avoir préalablement créé son Profil MConnect

a) Révocation des Certificats via l'Application MConnect Mobile

Pour révoquer ses Certificats, s'il a toujours accès à son Application MConnect Mobile avec ses données d'identité numérique, le Porteur peut réinitialiser son application de trois manières différentes :

- via le menu « Réglage », option « Réinitialiser MConnect Mobile » ;
- en sélectionnant l'option « Code déverrouillage oublié et réinitialisation de l'application » ;
- en supprimant l'application MConnect Mobile du téléphone mobile.

Les Certificats électroniques du Porteur sont alors révoqués.

b) Révocation des Certificats via le Profil MConnect

S'il a créé son Profil MConnect, le Porteur peut révoquer ses certificats depuis l'onglet Révocation (https://profil.mconnect.mc/revoke?lang=fr) de trois manières différentes :

- S'il a toujours accès à son Application MConnect Mobile, en choisissant l'option « Me connecter » et en confirmant la demande de révocation ;
- S'il n'a plus accès à son Application MConnect Mobile, en choisissant l'option « Accéder à la révocation ». Il devra alors avoir accès à l'un de ses moyens de contact (email ou téléphone), puis choisir l'option « code de révocation ». Il saisit son code de révocation et confirme la demande de révocation de ses Certificats ;

- S'il n'a plus accès à son Application MConnect Mobile et n'a plus son code de révocation, en choisissant l'option « Accéder à la révocation », puis l'option « questions secrètes ». Il renseigne alors les réponses aux 4 questions secrètes choisies lors de la création de son Profil MConnect, et confirme la demande de révocation de ses Certificats ;

Ces actions déclenchent la révocation par l'AC. Le numéro de série du certificat révoqué apparaîtra dans la prochaine LCR (Liste des Certificats Révoqués) publiée. Dans le cas d'une demande de révocation via le Profil MConnect, le Porteur, reçoit par courriel ou SMS une notification de la révocation. L'opération est enregistrée dans les journaux d'événements.

c) Révocation d'un certificat sans accès à l'Application MConnect Mobile ni au Profil MConnect :

Le Porteur contacte le support MConnect (https://mconnect.gouv.mc/aide), qui lui proposera un rendez-vous présentiel avec un Opérateur de l'AE DSN pour procéder à la révocation de ses certificats. Le Porteur devra se présenter au rendez-vous muni d'une pièce d'identité en cours de validité. Une fois la révocation effectuée par l'AE, un mail de confirmation est envoyé au Porteur.

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

d) 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 révocation 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 :

Le Porteur, s'engage à conserver l'Application MConnect Mobile et le code associé sous son contrôle exclusif de manière à préserver l'intégrité et la confidentialité de sa clé privée.

En conséquence, le code de déverrouillage de l'Application MConnect Mobile ne doit jamais être conservé en clair ni se trouver à proximité du téléphone mobile.

Le code 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 des Services Numériques.

Si une donnée communiquée par le Porteur 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 ou de la modification des données contenues dans le Certificat par le Porteur ou par la DSN, emporte obligation, à leur charge, de demander dans les meilleurs délais la révocation du Certificat associé.

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 DSN 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 DSN 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 NUMERIQUES 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 monégasques, 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 DSN 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 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 la signature électronique d'un document ne respecte pas les conditions de signature ou de cachet 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 du Certificat 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 DSN, 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/services-numeriques.

Le Porteur pourra être notifié par email ou SMS pour toute modification majeure des CGU. A défaut d'une manifestation de sa part dans un délai de 10 jours francs, la nouvelle version sera considérée comme ayant été acceptée.

10 LIMITES DE GARANTIES ET DE RESPONSABILITES

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

La DSN 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 DSN 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 DSN ne peut être engagée en cas de compromission de la clé privée. La DSN 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 DSN ne pourra être engagée dès lors que le Porteur 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 mentionnées au sein du dossier d'enregistrement.

Il s'agit notamment des informations :

Identité / Situation de famille

- Prénom(s)
- Nom de naissance
- Nom d'usage
- Date de naissance
- Ville de naissance
- Pays de naissance
- Sexe

Adresses et coordonnées

- Adresse e-mail
- Numéro de téléphone mobile

Données d'identification électronique

Données Certificats pour personne physique :

- Cn = NOM DE NAISSANCE-NOM D'USAGE (le cas échéant)–PRENOM(S)
- SerialNumber (identifiant unique)
- givenName=PRENOM(S)
- SurName=NOM DE NAISSANCE
- C=MC (country)
- L'Autorité de Certification
- La date de début de validité du certificat
- La date de fin de validité du certificat

La Direction des Services Numériques 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 DSN, 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 d'authentification ou de signature électronique sont collectées par l'État de Monaco (**Direction des Services Numeriques**) qui agit en qualité de responsable du traitement.

La Direction des Services Numériques exploite un traitement d'informations nominatives ayant pour finalité la Création d'une identité numérique monégasque pour les non-Monégasques et non-résident, et délivrance des certificats électroniques attenants.

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° n° 10.884 du 25 octobre 2024 portant modification de l'Ordonnance Souveraine n° 7.995 du 12 mars 2020 portant création de la Direction des Services Numériques, modifiée.
- 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 électronique d'authentification ou de signature électronique aux personnes non-monégasques et non-résidentes à Monaco 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, Moyens de contact, Réponses personnelles pour déblocage du code de révocation, 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 de la demande de certificat électronique d'authentification et de signature électronique pour les personnes non-monégasques et non-résidentes à Monaco ont un caractère obligatoire. A défaut du renseignement des mentions obligatoires dans le cadre du formulaire de demande, la demande de création de certificat électronique d'authentification et de signature électronique ou 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 électronique d'authentification ou de signature électronique, la personne concernée peut former une demande :

- En cliquant ici / En se rendant sur le site gouv.mc, Rubrique « Gouvernement et Institutions »/ Secrétariat Général du Gouvernement > Direction des Services Numériques > Coordonnées.
- A l'adresse postale suivante :

DIRECTION DES SERVICES NUMERIQUES
2 rue du Gabian
Immeuble "Les Industries"
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 des Services Numériques pour la délivrance de certificats aux personnes non-monégasques et non-résidentes à Monaco a fait l'objet d'une déclaration CCIN.

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.