TRUSTED NATIONAL INFRASTRUCTURE
PRINCE'S GOVERNMENT CERTIFICATION AUTHORITY

TERMS OF USE

Document status - Classification	Reference
Current - Public	2.16.492.1.1.1.1.3.3

Version	Date	Description
1.1	22/07/2021	Initial version
2.0	4/11/2021	Published version
2.1	08/12/2021	Published version
2.3	04/03/2022	Modified version
2.4	07/09/2022	Modified version

Table of contents

1 PURPOSE 2
2 DEFINITIONS 2
3 CONTACT DETAILS 3
4 USING THE CERTIFICATES 3
5 LIMITATION OF USE 4
6 CONDITIONS FOR OBTAINING AND USING THE CERTIFICATE 4
6.1 APPLICATION FOR CERTIFICATE AND SUPPORTING DOCUMENTS 4
6.2 ISSUANCE OF THE CERTIFICATE AND ACCEPTANCE 6
6.3 USE OF THE CERTIFICATES 7
6.4 RENEWAL OF CERTIFICATES 7
6.5 REVOCATION 8
7 OBLIGATIONS 9
8 LIABILITY 10
9 LIMITS OF GUARANTEES AND LIABILITY 11
10 DATA RETENTION 11

11 INTELLECTUAL PROPERTY 12
12 PROTECTION OF PERSONAL DATA 13
13 APPLICABLE LAW, DISPUTE SETTLEMENT 14
14 INDEPENDANCE OF THE PARTIES AND NON-DISCRIMINATION 14

1 PURPOSE

The purpose of these Terms of Use (or "Terms of Use for certificates", hereinafter referred to as "GTCs") is to set out the terms and conditions for the issue and use of electronic certificates for electronic signature and authentication issued by the Prince's Government (hereinafter referred to as the "Government") as well as the respective commitments and obligations of the various parties involved.

These GTCs apply to any Holder (resident), requesting the electronic certificates offered by the Government and using the said certificates.

The Holder (resident) confirms that he/she has read and understood the entirety of these GTCs before using the certificate and undertakes to adhere to them.

2 DEFINITIONS

The following words and phrases, beginning with a capital letter, in the singular or plural, are employed herein with the meanings specified below:

- **Agent (or Registration Operator):** refers to the Police Department operator in charge of processing requests to generate or revoke certificates.
- **Certification Authority or CA:** refers to all computer systems that allow the creation and revocation of electronic certificates. It operates under the responsibility of the Police Department.
- **Registration Authority or RA:** refers to the authority implemented by the Police Department, which carries out the following functions:
    - Receipt of certificate request files
    - Receipt of certificate revocation request files
    - Verification of the identity and the authorisation of the future Certificate holder
    - Triggering the generation of certificates
    - Delivery to the future Holder of the cryptographic device (smart card) required for their use
    - Processing the revocation of the certificates
    - Triggering the data archiving functions
- **Certificate:** refers to the public Key of a Holder, to which other information is associated. It corresponds to the private key issued by the certification authority.
- **Terms of Use or GTC:** means the present terms of use
- **Contract:** refers to the contractual framework made up of these GTCs, the certificate application file and the related Certification Policy shown at the following address:

https://mconnect.gouv.mc/gouvernement-princier applicable on the date of agreement of the contract

- **C2SC (Trusted Services Monitoring Committee):** This committee ensures compliance with the Certification Policy and consistency with other framework documentation.
- **Personal Data:** Any information relating to an identified or identifiable individual ("person concerned"). An "identifiable individual" is any individual who may be identified, directly or indirectly, including through reference to an identifying detail such as a name, an identification number, location data, an online username, or one or more attributes specific to his or her identity.
- **Applicant:** The Applicant is the natural person who applies to the Registration Authority to obtain a residence permit and an electronic certificate of a natural person.**Trusted National Infrastructure (TNI):** The TNI is the set of components, functions and procedures dedicated to the management of cryptographic keys and their certificates used by trusted services implemented by the Monaco Cyber Security Agency (AMSN) on behalf of the Prince's Government. The PRINCE'S GOVERNMENT CERTIFICATION AUTHORITY is one of the authorities attached to the TNI.

- **TNI Security Officer:** the person who is responsible, under the orders of his or her employing authority, for establishing the security rules and instructions to be implemented with respect to persons and protected information or media and for verifying their implementation.
- **Certification Policy or CP**: refers to the CP of the Prince's Government Certification Authority, document that establishes the principles that apply to the Certification Authority, and to all stakeholders involved in the lifecycle of a certificate, (which can be consulted at the following address: https://mconnect.gouv.mc/gouvernement-princier)
  The CP identifiers applicable to these GTCs are:
  - The CP of Root Certification authority: 2.16.492.1.1.1.1.1.1.
  - The CP of the Prince's Government Certification Authority: 2.16.492.1.1.1.1.3.1.
- **Holder:** refers to the holder of the residence permit and the user of the electronic certificates. This is the individual identified on the Certificate.
- **Registration Process** : refers to the process that consists of creating and managing the certificate application file;

3 CONTACT DETAILS

Requests for information regarding the issuance of residence permits and electronic Certificates provided by the Police Department can be made:

- By post: Police Department - Administrative Police Division, Stade louis II, entrée B, first floor, MC 98000 MONACO
- By email by completing the following form: https://service-public-particuliers.gouv.mc/Contactez-l-administration/(entite)/5348/(name)/5729

4 USING THE CERTIFICATES

The types of certificate issued enable:

- authentication of a Holder (natural person) on online services provided by public and private partners using their residence permit

- electronic signature of a Holder (natural person), allowing them to sign documents electronically using their residence permit
- authentication of a Holder (natural person) on online services provided by public and private partners using their smartphone
- electronic signature of a Holder (natural person) allowing them to sign documents electronically using their smartphone

The types of Certificates and uses are described in the CP of the Prince's Government Certification Authority (which can be consulted at the following address: https://mconnect.gouv.mc/gouvernement-princier).

5 LIMITATION OF USE

The Holders must strictly respect the authorised uses of the key pair and the Certificates. In the case of fraudulent use, they may be held responsible.

The authorised use of the key pair and the associated Certificate is specified in the Certificate itself.

The use of the Holder's private key and the associated Certificate, is strictly limited to the service defined by the identifier of his/her CP.

The Holder acknowledges that he/she has been informed that fraudulent use or use that does not comply with the present GTCs, as well as with the authorised use of the key pair and the Certificate, is a legitimate reason for revocation by the CA.

The use of Certificates is limited to the uses described in the CP of the Prince's Government Certification Authority which can be consulted at the following address: https://mconnect.gouv.mc/gouvernement-princier.

6 CONDITIONS FOR OBTAINING AND USING THE CERTIFICATE

The qualified certificate issuance service has been evaluated by an organisation accredited by the French Accreditation Committee (COFRAC). This service complies with the published CP.

6.1 APPLICATION FOR CERTIFICATE AND SUPPORTING DOCUMENTS

Appointments to register applications for residence permits and electronic authentication and signature certificates must be made with the Registration Authority: the Police Department (specifically the Residents Section).
Appointments with the Police Department can be made online using the online service, or directly at the office of the Residency Section of the Police Department.
The principles and conditions as well as a list of documents that need be provided are available on the public service website: https://service-public-particuliers.gouv.mc/Nationalite-et-residence/Residence
The certificate application registration service is available during the opening hours of the Residents Section.

6.1.1 *Registering an application for a residence permit or an application for an electronic certificate*

The reference text mentioned below sets out the visual and electronic content of the Monegasque residence permit.

Ministerial Decree no. 2021-430 of 17 June 2021 implementing the Article 4 of the Ordinance no. 3.153 of 19 March 1964 on the conditions of entry and residency for foreigners in the Principality, as amended

(See Articles 2, 3, 4, 6, 7 and 10)

An application for a residence permit constitutes an application for electronic authentication and signature certificates.

The issuing process includes the processing and coordination of all the necessary stages in the production of a final permit, from registration of the application for the permit to its issue to the Holder.

The following steps must be completed:

- Applicant visits the Police Department in person
- Verification of the identity of the applicant
- Biographical details noted
- Biometric information taken (photograph and fingerprints)
- Completion of application form for an electronic certificate linked to the digital identity. This document is called the enrolment receipt.

The application for electronic authentication and signature certificates takes the form of an enrolment receipt. This document is automatically generated by the system during the face-to-face application appointment between the registration operator and the holder.

The application document summarises the fields and data related to the holder. It is dated and signed by the operator and the holder, and subsequently kept by both parties.

- Acceptance of the GTCs (by signing the enrolment receipt)
- Review of application:
    - Checks to ensure that the application is complete
    - Verification of the applicant’s identity and legitimacy

6.1.2 *Processing of applications*

- Validation of the application by the registration operator (Police Department agent)
- Validation of complete application by the Police Department Director
- Generation of electronic certificates:
    - Electronic customisation of card: generation of certificates linked to the digital identity
    - Graphic customisation of card
- Quality check of card and electronic certificates by the registration operator: verification of biographic and biometric information, the MRZ, the electronic certificates and the ICAO container

6.2 ISSUANCE OF THE CERTIFICATE AND ACCEPTANCE

6.2.1 *Process for issuing electronic certificates loaded onto the residence permit*

- Applicant visits the Police Department in person
- Verification of biometric information (holder's fingerprints and identity)
- Tacit acceptance of certificate by the Holder (validation by the Holder of the electronic certificates) *
- Issuance of residence permit and certificates at face-to-face appointment
- Provision of an issuance slip containing a summary of the information related to the issue of the certificates and the cancellation code for the Holder

*Holders have 7 clear days from the date the residence permit is issued to verify that the content of the certificates delivered to them is correct (see mconnect.gouv.mc/logiciel), whether they have activated the means of identification by generating a PIN or not.

In the event of an error regarding the Holder's identity on the certificates, the Holder shall contact the Residents Section to request the issue of a new residence permit and new certificates.

6.2.2 *Process for activating the resources to use the Holder's digital identity*

The Holder can activate the resources for using his/her digital identity during issuance of their residence permit with the operator at the Residents Section, or at a later date using the interactive terminal available for self-service use at the Residents Section of the Police Department.

The Holder may decide to activate or not the means of identification.

The steps involved in activating the means associated with the digital identity (generation of a PIN) with the operator are as follows (after issuance process):

- A PIN pad (entry device) is made available to the Holder;
- A PIN* chosen by the Holder is entered (the PIN entered remains confidential; it is not displayed to the Holder nor the operator);
- Confirmation of chosen PIN by entering it a second time;
- Validation by the operator that the means of identification have been activated on the system (if the two PINs entered match)

The steps involved in activating the means of identification associated with the digital identity (generation of a PIN) on the self-service interactive terminal are as follows:

- The residence permit is read using the reader on the interactive terminal
- The option "Activate my digital identity" is selected on the screen
- Biometric verification of the Holder's identity using facial recognition (comparison of the photo on the ICAO chip with the Holder's face)
- A PIN* chosen by the Holder is entered (the PIN entered remains confidential; it is not displayed in clear on the screen.);

- Confirmation of chosen PIN by entering it a second time;
- Automatic validation by the interactive terminal that the resources for using the digital identity have been activated on the system (if the two PINs entered match)

**The code must not contain:*

- The same digit 5 times

- 5 consecutive digits

- 5 digits which are the same as the last 5 digits of the document number, in the same order

6.3 USE OF THE CERTIFICATES

All residence permits contain a cryptographic chip.

The chip contains two types of certificates:

- An authentication certificate
- An electronic signature certificate

The two certificates include the same fields:

- Last names and first names of the Holder
- Country of issuance
- Certificate serial number
- Certification Authority
- Valid from date
- Valid until (expiry) date

The electronic Certificates that allow the Holder to verify their identity or sign documents using their smartphone are derived from the electronic Certificates stored on the residence permit.

The Certificate shall only be used for the purposes defined in Article 4 of the present GTCs.

The authentication service on MCONNECT is available 24/7, 365 days a year, except in the event of force majeure, which will be announced on the following website: mconnect.gouv.mc.

Information messages are published on mconnect.gouv.mc website in the event of problems that could affect the integrity and availability of the service.

6.4 RENEWAL OF CERTIFICATES

The electronic certificates maximum lifetime is three (3) years.

The residence permits issued by the Police Department may have different validity periods depending on the category of residence permit issued:

- A "temporary" (temporaire) permit is valid for one year
- An "ordinary" (ordinaire) permit is valid for three years
- A "spouse of a Monegasque" (conjoint de monégasque) permit is valid for five years

- A "privilege" (privilégié) permit is valid for ten years

In the case of the “temporary” and “ordinary” categories, the renewal can be carried out alongside the application and issuance of a new residence permit and a new certificate.

For categories of residence permit that are valid for more than 3 years (“privilege” and “spouse”), the holder must renew the electronic certificates using the self-service option on the interactive terminal available in the Residency Section of the Police Department.

The Holder authenticates on the interactive terminal by entering his/her PIN and then renews the certificates directly on the terminal. The renewal process takes approximately 3 minutes and is effective immediately, allowing the electronic certificates to be used without the issuance of a new permit.

6.5 REVOCATION

The possible causes of a revocation are described in the CP of the Prince's Government Certification Authority (which can be consulted at the following https://mconnect.gouv.mc/gouvernement-princier).

The certificate revocation service is available 24/7, 365 days a year, except in the event of force majeure, which will be announced on the mconnect.gouv.mc website.

The certificates may be cancelled for the following reasons:

- Expiry of Certificate: electronic certificates are valid for three (3) years, following which they are automatically revoked
- Holder revocation request (the card is lost or stolen, or the Certificates have been compromised)

In the event that the card is lost or stolen and the certificates may have been compromised, the Holder should use the revocation code given on the same day as the permit was issued (recorded on the issue slip) to complete the revocation form which can be accessed online using this link: https://mconnect.gouv.mc/formulaire-de-demande-de-revocation-des-certificats-electroniques-pour-les-titulaires-de-carte-de-sejour. The holder will be notified by the Registration Authority that their certificates have been revoked.

Requests to revoke certificates must be made as soon as the relevant event becomes known.

If the revocation code has been lost, the Holder must visit the Police Department (Residency Section) in person to request the cancellation of the Certificates.

- **Issuance of a new permit: replacing the previous permit** and leading to the revocation of the electronic Certificates stored on the previous permit (e.g. permis renewal, permit duplicate, etc.)

- **Departure of the Holder from the Principality**, resulting in a Police Department member of staff taking action on the dedicated business application to invalidate the electronic Certificates. If the Holder has left the Principality or is no longer a resident, then their Certificate becomes invalid, and their digital identity can no longer be used.

In the event of departure from the Principality, any current online procedures being carried out using the Holder's electronic certificates will not be able to be completed since the certificates will have been revoked. Holders are therefore advised to save from the relevant online services any data and documents about them that they wish to save before providing notification of their departure from the Principality.

- **Death of Holder**, resulting in a Police Department member of staff taking action on the dedicated business application to invalidate the electronic Certificates.

- **Fraudulent use or failure to comply with these GTCs:** resulting in the revocation of certificates by the CA or the TNI Security Officer in accordance with Article 5 above. This request to revoke certificates may be made by the C2SC Manager.

Process for issuing the revocation code to the Holder:

When their residence permit is issued, all Holders (residents) receive an issuance slip.

The issuance slip contains the revocation code (in the format 123456).

The agent explains to the Holder that this slip must be carefully kept, and that the revocation code will be required to revoke their electronic certificates remotely.

Checking the status of a Certificate:

The Holder may check the status of his/her Certificates at any time by consulting the available CRL (Certificate Revocation List), or by asking the Online Certificate Status Protocol (OCSP), which features a "revoked certificate " response after the certificate's expiry date. Revoked certificates remain in the CRL even after their original expiration date. In the event of permanent cessation of CA activity, a final CRL will be issued with an end of validity date of 31 December 9999, 23h59m59s.

7 OBLIGATIONS

The Holder shall take all appropriate measures to ensure the security of their IT terminals on which the media (smart cards) are used.

The Holder shall install the Smart Card Manager software (available at this link: https://mconnect.gouv.mc/en/logiciel) to enable use of the electronic certificates.

The Administration bears no liability for use of this software.

The Holder shall ensure that their media and associated PIN code remain under their exclusive control to maintain the integrity and confidentiality of their private key.

Consequently, the PIN code must never be kept in clear text or be near the smart card.

The PIN code must never be disclosed under any circumstances. In the event of non-compliance with this obligation, the Holder will assume full responsibility for the consequences of such non-compliance without any recourse against the Police Department or the Prince's Government of Monaco.

When Police Department issues the permit, the permit complies with the security requirements set out in the relevant chapters of the CP.

When using the Electronic Signature Certificate, the Holder must ensure that he/she uses an up-to-date version of the Adobe Acrobat Reader DC software and must comply with the software's terms and conditions of use.

If any data provided by the Holder changes, the Holder must inform the Police Department immediately so that the recorded information can be updated, and a new residence permit issued if required.

Knowledge of proven or suspected compromise of confidential data, failure to respect the present general conditions, or modification of the data contained in the Certificate, by the Holder, or by the Police Department, entails an obligation, on their part, to request the revocation of the associated Certificate as soon as possible, due to the risk of identity fraud.

The Holder undertakes to no longer use a Certificate following its expiration, a request for revocation or notification of the revocation of the Certificate, whatever the cause.

The Holder undertakes to verify the use indicated in the Certificate.

Any recipient of a document signed by a Holder, can check whether the status of a Certificate has been revoked or not by checking the Certificates Revocation List indicated by the distribution point shown in the Certificate.

If the Certificate is revoked, it is the responsibility of the recipient of the signed document to determine whether or not it is reasonable to trust the Certificate. The Police Department shall not be liable in any way for revocation of the Certificate.

Obligations of the CA:

In the event of a revocation request by the Holder, the Police Department shall revoke the Certificate within less than twenty-four (24) hours of a request by the applicant.

The conditions for ending relations with PRINCE'S GOVERNMENT CERTIFICATION AUTHORITY are published in paragraph 4.11 of the CP.

8 LIABILITY

Certificates must not be used in an abusive or malicious manner.

The Holder undertakes to use the Certificates:

- In compliance with the laws and regulations of Monaco, and the rights of third parties
- Fairly and in accordance with their use
- At their own risk

The Holder acknowledges and accepts that the Police Department cannot be held responsible in connection with its issuing of certificates, particularly in the event of alteration, any illicit or prejudicial use of the Holder or a third party in the network by a third party.

The Holder assumes full responsibility for any consequences resulting from his/her faults, errors, or omissions.

The Holder confirms to the Administration that he/she is the owner of the documents that he/she signs using the Electronic Signature Certificate

The Administration is not responsible for the legality and conformity of the documents signed through its Service using the Electronic Signature Certificate.

The Administration is not responsible if the electronic signature of a document does not comply with the signature requirements for this type of document.

The Holder is solely responsible for the life cycle of the documents he/she signs from their creation to the end of their storage.

The Holder shall refrain from using or attempting to use the Certificate, functions and authorised uses of key pairs for any purpose other than those provided for herein and by the Certificate itself.

The terms of these GTCs may also be amended at any time, without prior notice, according to modifications made by the Police Department, changes in legislation or any other reason deemed necessary. It is the Holder's responsibility to inform him/herself of the said term.

The version of the GTCs which takes precedence is the one available on the publication site https://mconnect.gouv.mc/gouvernement-princier

9 LIMITS OF GUARANTEES AND LIABILITY

Under no circumstances does the Police Department intervene, in any way whatsoever, in the contractual relations that may be established between the Holders of the said Certificates.

The Police Department does not assume any commitment or responsibility as to the form, sufficiency, accuracy, authenticity, or legal effect of the documents submitted at the time of the application for a Certificate.

The Police Department assumes no responsibility or liability for the consequences of any delay or loss in the transmission of any electronic message, letter, or document, or for any delay, corruption, or other error that may occur in the transmission of any electronic communication.

The Police Department cannot be held responsible for compromise of the private key. The Police Department is not entrusted with the storage and/or protection of the private key of the Certificate.

The parties expressly agree that the Police Department cannot be held liable in any way if the Holder has not requested the revocation of the Certificate in accordance with the provisions of this document.

10 DATA RETENTION

Data is kept during the creation of the registration file as soon as the request to provide the residence permit and therefore supply a certificate is received.

Personal information is the nominative information of the Holder mentioned in the registration file.

This information includes the following:

Civil status

- Surname

- First names
- Preferred name
- Date and time of birth
- Place of birth
- Sex at birth
- Initials (e.g. JEAN DUPOND, JD)

Address and contact information

- Postal address

Electronic identification data

- ICAO container data: MRZ

Electronic authentication and signature certificate data

- Surnames and first names of the Holder
- Country of issuance
- Certificate serial number
- Certification Authority
- Valid from date
- Valid until (expiry) date

Biometric data

- Photograph
- Digital fingerprints

Signature

- Handwritten signature (signed on a pad)

Data relating to the application and the card

- Application number
- Card number
- Valid to/from date
- Issuing authority
- CAN (card access number for recovery of PUK)

Applications for sovereign identity cards are retained indefinitely as historical archives.

The technical logs are retained in a secure area for one year, then deleted.

Data is retained in compliance with the appropriate level of protection for personal data, management of which is covered in paragraph 12.

11 INTELLECTUAL PROPERTY

The trademarks and/or logos owned by the Police Department, appearing on all media, are trademarks protected by the legal provisions applicable in Monaco.

Any representation or reproduction, whether total or partial, is prohibited and constitutes a criminal offence that will be punished by the Monaco courts, unless express permission is obtained from the Administration.

12 PROTECTION OF PERSONAL DATA

As part of the process of creating a digital identity in Monaco, the State of Monaco/Police Department processes personal data for the purpose of "Managing a platform to issue and administer residence permits".

The personal data collected during processing is gathered indirectly and comes from the individual concerned (in the case of the photo and fingerprints) or the source file that constitutes the database relating to residents of the Principality.

The sole recipients of the data are authorised Police Department staff.

In accordance with the applicable provisions on protecting personal data in the Principality of Monaco, the individuals affected by this processing have a right to access their personal data, and to request the correction, updating or removal of erroneous, incomplete, or outdated data. To exercise their rights, the individuals concerned can submit a written request setting out the subject of their request, as well as their surname, first name and date of birth, by post to the following address:

Direction de la Sûreté Publique

Stade louis II, entrée B, étage 1

MC 98000 MONACO

To ensure that the response remains confidential and that the reply is sent only to the person whose data is involved, the applicant may be asked to supply proof of identity, in black and white.

The technical solution used by Police Department to issue electronic certificates has been approved by the Data Protection Authority of Monaco (Commission de Contrôle des Informations Nominatives – 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 APPLICABLE LAW, DISPUTE SETTLEMENT

The parties expressly agree that only Monegasque legislation and regulations are applicable.

They undertake to seek an amicable agreement in the event of a dispute. At the initiative of the requesting party, a meeting will be held. Any agreement to settle the dispute must be recorded in writing on a document signed by an accredited representative of both parties.

In the event of a dispute relating to the interpretation, formation or performance of the Contract and failing to reach an amicable agreement, the parties hereby give express and exclusive jurisdiction to the competent courts of the Principality of Monaco.

14 INDEPENDANCE OF THE PARTIES AND NON-DISCRIMINATION

The organization implemented by the CA is dedicated to its activities and ensures the separation of roles. It preserves the impartiality of operations and ensures that the trusted activities provided are undertaken in an equivalent manner for all beneficiaries who have accepted the general conditions of use of the service and who respect the obligations incumbent upon them.

Wherever possible, the CA shall implement appropriate approaches to make its service accessible to all persons, including those with disabilities, considering the specificities of each applicant on a case-by-case basis.

In general, the services provided by the CA such as, but not limited to, certificate generation, revocation management and certificate status are performed independently and are therefore not subject to any pressure.