Mairie de Monaco

Service Informatique

TRUSTED NATIONAL INFRASTRUCTURE MONACO CITY HALL CERTIFICATION AUTHORITY

TERMS OF USE

Document Status - Classification	Reference
Current - Public	2.16.492.1.1.1.1.2.3

Version	Date	Description
1.1	10/12/2021	Initial version
1.3	04/03/2022	Modified version
1.4	08/09/2022	Modified version

Table of contents

1. Purpose 2
2. Definitions 2
3. Contact details 3
4. Types of Certificates and Uses 3
5. Limitation of Use 4
6. Conditions for obtaining and using the Certificate 4
   - **6.1** – Application for Identity Card and supporting documents 4
   - **6.2** – Issue of Identity Card and acceptance 5
   - **6.3** – Use of the Certificate 5
   - **6.4** – Activation of resources required to use the certificates stored on the identity card 5
   - **6.5** – Renewal of certificates 5
   - **6.6** – Cancellation of the certificate 6
7. Obligations 6
8. Liability 7
9. Limits of guarantees and liability 8
10. Data retention 8
11. Intellectual property 9
12. Protection of personal data 9
13. Applicable Law, dispute settlement 11
14. Independence of the parties and non-discrimination 11

1. Purpose

The purpose of these Terms of Use (or hereinafter referred to as "GTC") is to set out the terms and conditions for the issuance and use of electronic signature and authentication certificates issued by Monaco City Hall (hereinafter referred to as “City Hall”) as well as the respective commitments and obligations of the various parties involved.

The Monaco national identity card contains a cryptographic chip on which electronic certificates are stored.

These GTCs apply to any Applicant requesting a Monaco national identity card.

The Holder, or his or her legal representative, 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:

- **(Registration) Agent:** refers to the City Hall operator responsible for handling the functions defined below (Registration Authority).
- **Authentication:** process by which an IT system verifies the identity of a Holder.
- **Certification Authority or CA:** refers to all computer systems that allow the creation and revocation of Electronic Certificates.
- **Registration Authority or RA:** refers to City Hall, which carries out the following functions:
  - Receiving applications for identity cards on which certificates are stored
  - Verifying the identity and the authorisation of the future Certificate Holder
  - Triggering the generation of certificates
  - Delivering to the future Holder the cryptographic media required to use the certificates
  - Receiving requests to revoke certificates
  - Processing the revocation of the certificates
  - Triggering the data archiving functions
- **Certificate:** public key of a Holder, concatenated with other information made impossible to forge by signature with the private key of the Certification Authority that issued it.
- **C2SC (Trusted Services Monitoring Committee):** This committee ensures compliance with the Certification Policy and consistency with other framework documentation.
- **Terms of Use or GTC:** means the present terms of use.
- **Applicant:** The Applicant is the natural person who applies to a Registration Authority to obtain a certificate of a natural person.
- **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.

- **Trusted National Infrastructure or 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 City Hall 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 document that establishes the principles that apply to the Certification Authority, and to all participants in the entire lifecycle of a certificate (which can be consulted at the following address: https://mconnect.gouv.mc/mairie)

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 City Hall Certification Authority: 2.16.492.1.1.1.1.2.1.

- **Registration Process:** refers to the registration process that consists of creating and managing the certificate application file.

- **Legal representative:** refers to the person (or persons) legally designated to represent and protect the interests of a minor child or protected adult. Legal representatives act for and on behalf of the individuals they represent.

- **Electronic signature:** electronic data which is logically attached to or associated with other electronic data, and which the signatory uses to sign documents.

- **Identity document:** refers to the identity card on which the Certificate is stored.

- **Holder:** refers to the holder of the identity card, the individual identified in the Certificate.

3. Contact details

Requests for information regarding the issuance of Electronic Certificates provided by the City Hall can be made contacting:

Service de l'Etat Civil – Nationalité

(City Hall Registry Office –Nationality)
Place de la Mairie
98000 Monaco

Phone: (+377) 93 15 28 10 ou 93 15 28 16
Email: nationalite@mairie.mc

4. Types of Certificates and Uses

The types of Certificates issued are as follows:

- Authentication Certificates for individuals enable the Holder to use their identity card to verify their identity when logging into online services provided by public authorities and private partners.
- Electronic Signature Certificates for individuals enable the Holder to sign documents electronically using their identity card.
- Authentication Certificates for individuals enable the Holder to use their smartphone to verify their identity when logging into online services provided by public authorities and private partners.
- Electronic Signature Certificates for individuals enable the Holder to sign documents electronically using their smartphone.

The types of Certificates and uses are described in the PC of the City Hall Certification Authority (which can be consulted at the following address: https://mconnect.gouv.mc/mairie)

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 this website.

Notifications are made on the reference site mconnect.gouv.mc in the event of problems that could affect the integrity and availability of the service.

5. Limitation of Use

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

The authorized 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 authorized use of the key pair and the Certificate, is a legitimate reason for cancellation by the CA.

The use of Certificates is limited to the uses described in the Certification Policy for of the City Hall Certification Authority (which can be consulted at the following address: https://mconnect.gouv.mc/mairie).

6. Conditions for obtaining and using the Certificate

6.1 – Application for Identity Card and supporting documents

Applications for identity cards with a Certificate should be made to the Registration Authority (City Hall) using a registration form.

Applications are processed at an appointment with the City Hall Registry Office – Nationality during the office's opening hours.

The principles and conditions as well as a list of documents you will need to provide are available here: https://www.mairie.mc/poles/cadre-de-vie/nationalite-documents/la-carte-d-identite-monegasque-cime

The issue of an identity card with a Certificate 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 or their legal representative.

The identity document is created using an unchartedcard with electronic personalization (component including a Doc Signer responsible for the digital signature of the permit's ICAO data). For the digital identity part of the identity card, data certification is managed by the trusted national infrastructure.

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

6.2 – Issuance of Identity Card and acceptance

The issuance of the identity card to the Holder or their legal representative entails tacit acceptance of the electronic certificates stored on the card. The Holder has ten (10) clear days from the date they collect their card to check the information on the certificates stored on the card using the procedure described at https://mconnect.gouv.mc

6.3 – Use of the Certificate

All identity cards contain a cryptographic chip on which two types of certificate are stored:

- An authentication certificate
- An electronic signature certificate

The two certificates include the same fields:

- Last names and first names of the Holder
- Issuing country
- 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 identity card.

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

6.4 – Activation of resources required to use the certificates stored on the identity card

If the Holder wishes to activate the resources to use their digital identity, they will need to enter a five-figure PIN of their choice, either when they collect their identity card or at a later stage, usingan interactive terminal.

6.5 – Renewal of certificates

All electronic certificates are issued for a maximum of three (3) years and no longer than the expiry date of the identity card.

Identity cards issued by City Hall are valid for five (5) years.

The Holder may renew the certificates associated with their digital identity (preferably) before the three (3) years expire.

To do so, the Holder should use the interactive terminals at City Hall or at the Police Department and follow the steps shown on the screen. However, if the identity card has expired, an application for a new identity card containing new certificates will need to be made to the City Hall Registry Office – Nationality.

6.6 – Revocation of the certificate

The possible causes of a revocation are described in the CP of the City Hall Certification Authority (which can be consulted at the following address: https://mconnect.gouv.mc/mairie). 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 website MConnect.

The certificates may be revoked for the following reasons:

- **Expiry of Certificate:** electronic certificates are valid for three (3) years, following which they are automatically revoked.

- **Holder or their legal representative request revocation:** in the event that the card is lost or stolen, or erroneous information appears in the certificates, or the certificates have been compromised, for example.

  In the event that their permit is lost or stolen and their certificates may have been compromised, or if erroneous information appears in the certificates, the Holder or their legal representative should use the revocation code sent 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-d-identite

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

  A member of City Hall staff handles revocation requests received via the above-mentioned form on a daily basis and triggers the revocation of the certificates. The staff member then confirms to the Holder or their legal representative that their certificates have been revoked.

  If the revocation code has been lost, the Holder or their legal representative must contact the City Hall Registry Office – Nationality.

- **Issuance of a new permit:** replacing the previous permit and leading to the revocation of the electronic certificates stored on the previous permit.

- **Death of Holder:** resulting in a City Hall 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.

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 identity card readers are used.

The Holder shall install the Smart Card Manager software to enable use of the electronic certificates. The version of the software to be installed can be found on the website mconnect.gouv.mc at https://mconnect.gouv.mc/logiciel.

The Holder shall ensure that the version of the operating system they are running is compatible with the requirements of the software to be installed.

The Holder shall ensure that their identity card and associated PIN 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 Identity 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 City hall or the Prince's Government of Monaco.

When City Hall 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.

In the event of a change to the information sent via the registration form, the Holder or their legal representative will need to inform City Hall immediately so that this can be updated, and a new identity document 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 City Hall, 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.

In the event of a revocation request by the Holder or their legal representative, the City Hall shall cancel the Certificate within less than twenty-four (24) hours following receipt of the request, after confirming the identity of the Holder.

The conditions for ending relations with the City Hall 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 City Hall cannot be held responsible for the Certification service, 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 City Hall that he/she is the owner of the documents that he/she signs using the Electronic Signature Certificate.

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

The City Hall 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 Certificate 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 City Hall, 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/mairie

9. Limits of guarantees and liability

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

The City Hall 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 City Hall 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.

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

The parties expressly agree that the City Hall 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 identity card 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

- Title
- Surname
- Preferred name
- Three first names
- Nationality
- Date and place of birth
- Sex

Address and contact information
- Full Adress
- Email /Phone

Electronic identification data
- Digital identity certificates
- ICAO certificates

Biometric data
- Photograph
- Two digital fingerprints
- Digitised handwritten signature

Time information: timestamps, etc.
- Login information for City Hall Registry Office-Nationality staff
- Login information for the supplier's administrators

Data retention is undertaken in compliance with the level of protection appropriate to the personal data whose management is the subject of paragraph 12.

The technical logs are kept in a secure space for a period of one year and are then erased.
Applications for sovereign identity cards are retained for an unlimited length of time as historical archives.

11. Intellectual property

The trademarks and/or logos owned by the City Hall, 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 City Hall.

12. Protection of personal data

In accordance with the Act no. 1.165 of 23 December 1993 on personal data protection, amended, personal data collected during the process of issuing a Monaco national identity card is collected by Monaco City Hall in its capacity as the data controller.

Dans In this respect, Monaco City Hall processes personal data for the purpose of "Managing the operations required to create and issue Monaco national identity cards." This processing makes it possible to:

- Create, produce, and issue Monaco national identity cards
- Check the existence of a digital identity before enrolment
- Activate the Certificate enabling use of the digital identity

The treatment carried out on 22 June 2021 is justified by compliance with a legal obligation incumbent on Monaco City Hall in accordance with the provisions of Act No. 959, dated 24 July 1974, on the Organisation of the Commune, as amended, and the associated implementing legislation.

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. The right to request that data is updated and corrected will be covered by the request for a new Monaco national identity card.

To exercise their rights or in the event of any questions about how their personal data is processed in connection with the issue of Monaco national identity cards, the individuals concerned can submit a written request to the City Hall data protection officer, setting out the subject of their request, as well as their surname, first name and date of birth, by post to the following address:

Mairie de Monaco – Service Informatique
A l'attention du D.P.O.
3, rue Philibert Florence
98000 MONACO

The individuals concerned may also contact the Monaco City Hall data protection officer via email using the address: dpo@mairie.mc.

To ensure that the response remains confidential and that the reply is sent only to the person whose data is involved, those submitting requests may be asked to prove their identity.

In addition, the Prince's Government carries out the following automated processing of personal data, which is required to issue the electronic certificates stored on the identity card chip and linked to the digital identity, and is interconnected to the processing carried out by Monaco City Hall:

- "Management of digital identities using the Monegasque National Digital Identity Register (RNMIN) operated by the Digital Services Department.

- "Management of resources for using the digital identity recorded on Monaco national identity cards and residence permits (Certificates, CAN and PUK code)", (CLCM), operated by the Digital Services Department.

- "Supply of trusted services for digital identity (MConnect and MConnect Mobile) operated by the Digital Services Department.

- "Platform for activating and managing digital identity following issue of the permit" (kiosk) operated by the Digital Services Department.

The technical solution used by City Hall to issue electronic certificates has been approved by the Data Protection Authority of Monaco (Commission de Contrôle des Informations Nominatives – CCIN)

- Délibération n° 2021-108 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 opérations nécessaires à l'établissement et à la délivrance de la Carte d'Identité Monégasque » présenté par la Commune de Monaco.
- Délibération n° 2021-106 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 « Fichier des Nationaux et de leur famille », présentée par la Commune de Monaco.
- 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

It is expressly agreed that only Monegasque legislation and regulations are applicable.

In the event of a dispute, the competent courts of the Principality of Monaco have express and exclusive competence.

14. Independence 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, certificate generation, revocation management and certificate status are performed independently and are therefore not subject to any pressure.