TRUSTED NATIONAL INFRASTRUCTURE
ADMINISTRATIVE SERVICES CERTIFICATION AUTHORITY
TERMS OF USE

Document Status - Classification	Reference
Current - Public	2.16.492.1.1.1.1.5.3

Version	Date	Description
1.0	4/11/2021	Initial version
1.1	04/03/2022	Modified version
1.2	30/08/2022	Modified version

Table of contents

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, authentication, and electronic seals certificates, offered by the Human Resources and Training Department (hereinafter referred to as the "DRHFFP" or "HRD") as well as the respective commitments and obligations of the various parties involved.

These GTCs apply to any Applicant, belonging to a Administrative Services, requesting the electronic certificates offered by the HRD and using the said certificates.

The Holder, respectively the Certificate Manager, 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:

- **Certification Authority or CA**: refers to all computer systems that allow the creation and revocation of electronic certificates.
- **Registration Authority or RA**: refers to the HRD.

It performs the following functions:

  - Receipt of certificate generation request files
  - Receipt of certificate revocation request files
  - Verification of the identity and the authorisation of the Certificate Applicant
  - Delivery to the future Holder, Certificate Manager (CM) if applicable, of the cryptographic media for use of the corresponding certificates
  - Delivery to the future CM of the corresponding electronic seals certificates
  - Triggering the generation of certificates
  - Certificates revocation treatment
  - Triggering the data archiving functions.

- **Certificate:** refers to the public Key of a Holder, respectively a CM, with 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**: The contractual whole, comprised of the present GTC, the certificate application file and the related Certification Policy shown at the following address: https://spp.gouv.mc/services-administratifs applicable on the date of agreement of the contract.
- **Applicant:** The Applicant is the natural person who applies to a Registration Authority to obtain a certificate of a natural person or an electronic seal.
- **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 (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 Administrative Services Certification Authority is one of the authorities attached to the TNI.

- **Authorised Representative**: the individual who has received a mandate from a future holder, or a future CM, to manage the certificate's lifecycle.
- **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.
- **Registration Operator**: refers to the HRD operator in charge of processing certificate application files.
- **Holder**: refers to the Certificate Holder, a natural person identified in the certificate.
- **Certification Policy or CP**: the CP of Administrative Services Certification Authority refers to the document that establishes the principles that apply to the Certification Authority, to legal entities, Authorised Representatives and Holders, respectively CMs, involved in the entire lifecycle of a certificate, (which can be consulted at the following address: https://spp.gouv.mc/services-administratifs)
  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 Administrative Services Certification Authority: 2.16.492.1.1.1.1.5.1
- **Registration Process**: refers to the registration process that consists of creating and managing the certificate application file.
- **Certificate Manager of the legal entity or CM:** The concept of Certificate Manager applies only to final certificates of legal entities. The Certificate Manager is the natural person appointed and mandated by the Legal Representative of the legal entity to manage all or part of the legal entity's electronic seal certificates.

3 CONTACT DETAILS

Requests for information regarding the issuance of electronic certificates provided by the HRD can be made:

- By post:

Direction des Ressources Humaines et de la Formation de la Fonction Publique
3° étage - Stade Louis II - Entrée H
1 avenue des Castelans
BP 672
98014 MONACO CEDEX

- By email: esign-services-administratifs@gouv.mc

4 TYPES OF CERTIFICATES AND USES

The types of certificates issued by the HRD to Administrative Services are as follows:

- Signature certificates, issued on smart cards and used by individuals representing legal entities (in this case, officials at Administrative Services) to sign documents electronically
- Authentication Certificates, issued on smart cards and used to log into the portal for managing electronic certificate requests
- Certificates for electronic seals that can be delivered on a smart card or emailed to the Certificate Manager (server electronic seal).

The types of Certificates and uses are described in the CP of the Administrative Services Certification Authority, which can be consulted at the following address: https://spp.gouv.mc/services-administratifs.

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

5 LIMITATION OF USE

The Holders, respectively the CMs, 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, respectively the CM, and the associated Certificate, is strictly limited to the service defined by the identifier of his/her CP.

The Holder, respectively the CM, 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 Certification Policy of tthe Administrative Services Certification Authority at the following address: https://spp.gouv.mc/services-administratifs..

6 CONDITIONS FOR OBTAINING AND USING THE CERTIFICATE

6.1 APPLICATION FOR CERTIFICATE AND SUPPORTING DOCUMENTS

The registration service offered by the Administrative Services Certification Authority is available, by appointment, during the opening hours of the HUMAN RESOURCES AND TRAINING DEPARTMENT.

An application for a Certificate must be made to the HRD RA by means of a registration file.

The Registration Process consists of creating and managing the Certificate application file.

Registration requires a prior appointment with a Registration Operator.

Email submission of PDF forms by the Applicant

The Applicant may request Certificate application forms from the HRD by writing to the following address: esign-services-administratifs@gouv.mc.

The Applicant must return the completed forms to the HRD by email (esign-services-administratifs@gouv.mc) and will then be offered an appointment by a Registration Operator.

Receipt of PDF forms by email by the Registration Operator

A Registration Operator from the HRD will check applications received at the email address esign-services-administratifs@gouv.mc daily.

He will ensure that the forms attached are complete.

Forms must be completed directly in the PDF, to enable the Registration Operator to enter the data easily into the online administration tool.

If a form is incomplete or missing, he will reply to the applicant (by email) requesting additional information.

If the form is complete, the Registration Operator will offer the Applicant an appointment to proceed with registration.

6.2 PROCESSING OF APPLICATIONS

Verification and confirmation of the identity of the Holder, respectively the CM:

- The Holder, respectively the CM, submits his (paper) form, signed and stating acceptance of these GTC (with the GTC box checked)
- The HRD confirms the identity of the Holder, respectively the CM, by checking:
- The identity document of the Holder, respectively the CM, (identity card, passport, or residence permit)
- The Applicant's legitimacy, by consulting the register of persons with electronic signature authorisation. In addition, the HRD may check the Applicant's personnel number in its job tool (central site) by comparing it with the personnel number indicated on the form.

After conducting these checks, the HRD is ready to generate the smart card containing the electronic signature or electronic seal certificate, or the server electronic seal which will be sent by email.

Production of the card

The HRD produces the smart card containing the electronic certificate, where applicable.

6.3 ISSUANCE OF THE CERTIFICATES

Concerning Certificates for natural persons:

- Issuance of the Certificates by the Registration Operator face to face with the Holder
- The Holder is asked to validate the content of the certificate during the quality control carried out by the registration Operator. The certificate is thus explicitly accepted by the Holder at the time of delivery
- Signature of the certificate issuance document. This document is archived in the Holder's registration file

For Electronic seal Certificates:

- Issuance of the certificates by the Registration Operator face to face with the CM or by email, in the case of a server electronic seal
- The CM is required to validate the content of the electronic seal during its implementation
- Signature of the certificate delivery document. This document is archived in the CM's registration file.

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.

6.4 RECEIPT AND GENERATION OF THE PIN CODE AND REVOCATION CODE

Once the electronic certificates have been generated, three actions are taken:

- A paper letter containing the access code is immediately printed by the Registration Operator
- An automatic email containing an activation URL is sent to the Holder, respectively the CM
- An automatic email containing the revocation code is also sent to the Holder, respectively the CM

The access code, also called the activation code, enables the Holder, respectively the CM, to generate his 6-digit PIN code by clicking the URL in the email received. A PDF document containing the PIN code is then generated, and the Holder, respectively the CM must store it carefully (PIN codes cannot be chosen or changed).

Important information about the activation code and PIN code:

Until the Holder, respectively the CM has activated the link, the after-sales operator can return the email (only to the email address contained in the certificate).

Once the Holder, respectively the CM has clicked the link and entered the activation code, he will access a link to download the PDF containing his PIN code. He can click the link that generates the PDF only within the next 24 hours.

If the Holder, respectively the CM, with his card, enters the activation code but not the PIN code as required, the operation will fail after five attempts. In this case, the Registration Operator will have to generate a new electronic certificate on a new smart card.

The Registration Operator must therefore clearly explain the activation process and the distinction between the activation code and the PIN code.

6.5 USE OF THE CERTIFICATE

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

6.6 RENEWAL OF CERTIFICATES

The Certificate is valid for three (3) years.

The Holder, respectively the CM, and the Authorised Representative will be notified by the RA of the imminent expiration of their Certificate by email 45, 30 and 15 days before the expiration date.

The procedure for processing a request for a new Certificate is the same as for the first Certificate.

Any modifications made to the body of documents (notably the CP and the GTCs) in relation to that which prevailed when the previous Certificate was issued are made available to the Holder, respectively the CM, who can consult the dedicated website.

In all cases, the GTCs must be read and accepted.

6.7 REVOCATION

The possible causes of a revocation are described in the CP of the Administrative Services Certification Authority.

The revocation request must be made as soon as the corresponding event is known.

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.gouv.mc.

- Revocation of a certificate using the revocation code:

The self-service revocation process by the Holder, respectively the CM is carried out online in the following manner:

- The Holder, respectively the CM, connects to the revocation URL https://fo.certinomis.com/pro, "Cancel a certificate" button
- He/she enters his/her revocation code, which appears in an email notification received after, activation of his certificate (if applicable)
- He/she selects the certificate to be cancelled, as well as a reason for revocation
- This triggers the revocation by the CA. The serial number of the cancelled certificate will appear in the next CRL (Certificate Revocation List) published
- The Holder, respectively the CM, receives notification of the revocation by email
- The operation is recorded in the event logs

The Holder, respectively the CM, can, if necessary, be replaced by the Authorised Representative as soon as the revocation code is known in a legitimate way.

- Revocation of a certificate in the event of loss of the revocation code:

The Holder, respectively the CM, may have lost his/her revocation code. The Authorised Representative may wish, for legitimate reasons, to cancel a certificate (due to dismissal, departure, retirement, illness, etc.).

In this case, the applicant, whether he/she is the Holder, the Certificate Manager of a legal entity or the Authorised Representative, must go in person to the HUMAN RESOURCES AND TRAINING DEPARTMENT during working hours and days with a valid identity document or contact the Agency by telephone.

Authentication of the person by telephone is undertaken by means of answers to the 4 personal questions (among the 7) that the applicant will have filled in when submitting his/her registration file.

Revocation requests are processed within 24 hours of the request being taken into account.

- Revocation of a certificate by the RA or the TNI Security Officer:

The RA or the TNI's Security Officer may cancel a certificate, in particular in the event of suspected or proven compromise of the private key of the certificate, or in the event of fraudulent use or use that does not comply with the GTCs. The request for revocation may also arise from the C2SC Manager.

- Consulting the status of a Certificate:

The Holder, respectively the CM, 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 Service (OCSP), which features a "certificate cancelled" response after the certificate's expiry date. Cancelled 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

Obligations of the Holder, respectively the CM, and the Authorised representative:

The Holder, respectively the CM, is obligated to take all specific steps to ensure the security of his computer workstations on which the media (smart card) are used. Where the HRD provides the medium, it must be compliant with the security requirements stipulated in the relevant chapters of the CP.

The Holder, respectively the CM, undertakes to keep the equipment, whatever it may be, and the associated PIN code under his/her exclusive control to preserve the integrity and confidentiality of his/her 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, respectively the CM, will assume full responsibility for the consequences of such non-compliance without any recourse against the DRH.

In the case of a server electronic seal, the CM undertakes to generate the CSR and then to keep the private key under his/her exclusive control to preserve its integrity and confidentiality.

The Holder, respectively the CM, must ensure that he/she uses an up-to-date version of the Adobe Acrobat Reader DC software.

If any data communicated by the Holder, respectively the CM, or the Authorised Representative changes (e-mail address, etc.), the Holder must inform the CA without delay in order to update the registered file

Knowledge of proven or suspected compromise of confidential data, failure to respect the present general conditions, the death of the Holder, respectively the CM, or modification of the data contained in the Certificate, by the Holder, respectively the CM, or by the DRH, entails an obligation, on their part, to request the revocation of the associated Certificate as soon as possible

The Holder, respectively the CM, 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, respectively the CM, or the Authorised Representative undertakes to verify the use indicated in the Certificate.

Any recipient of a document signed by a Holder, respectively the CM, can check whether the status of a Certificate has been cancelled 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 it is reasonable to trust the Certificate or not. The DRH 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, respectively the CM, the DRH shall revoke the Certificate within less than twenty-four (24) hours of a request by the applicant.

The conditions for ending relations with the Administrative Services 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, respectively the CM, 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, respectively the CM, acknowledges and accepts that the DRH cannot be held responsible for its certificate issuance activity, particularly in the event of alteration, any illicit or prejudicial use of the Holder, respectively the CM, or a third party in the network by a third party.

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

The Holder, respectively the CM, ensures the Administration that he/she is the owner of the documents that he/she signs or seals using the Service.

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

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

The Holder, respectively the CM, is solely responsible for the documents life cycle that he/she signs or seals: from their creation to the end of their storage.

The Certificate Holder, respectively the CM, shall refrain from using or attempting to use the Certificate 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 DRH, changes in legislation or any other reason deemed necessary. It is the Holder's, respectively the CM, responsibility to inform him/herself of the said terms.

9 LIMITS OF GUARANTEES AND LIABILITY

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

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

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

DATA RETENTION

Data is kept during the creation of the registration file as soon as the request to provide a Certificate is made.

Personal information is the nominative information of the Holder, respectively the CM, and the Authorised Representative mentioned in the registration file.

This data is kept for ten (10) years. The storage period is seven (7) years after the expiration date of the Certificate (the lifetime of a Certificate is three (3) years).

This data is kept in a secure space by CERTINOMIS in compliance with the General Data Protection Regulation (GDPR). For more information, please visit: https://www.certinomis.fr/mentions-legales.

The AMSN has an agreement with CERTINOMIS to access this information in compliance with the GDPR.

The Human Resources and Training Department keeps the registration files in a paper format for seven (7) years after the expiration date of the Certificate in a secure space within the RA.

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

The technical solution used by the HRD to issue certificates to State actors is the same as that used by the Business Development Agency to issue certificates to companies. This solution has been declared to the CCIN, which issued a favourable opinion.

10 INTELLECTUAL PROPERTY

The trademarks and/or logos owned by the DRH, 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.

11 PROTECTION OF PERSONAL DATA

The technical solution used by the Human Resources and Training Department to issue certificates to State actors is the same as that used by the Business Development Agency to issue certificates to companies. This solution has been declared to the CCIN, which issued a favourable opinion.

12 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.

13 INDEPENDENCE OF THE PARTIES AND NON-DISCRIMINATION

The organisation 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.