TRUSTED NATIONAL INFRASTRUCTURE BUSINESS CERTIFICATION AUTHORITY

TERMS OF USE

Document Status - Classification	Reference
Current - Public	2.16.492.1.1.1.1.4.3

Version	Date	Description
1.0	16/03/2021	Initial version
2.0	4/11/2021	Modified version
2.2	04/03/2022	Modified version
2.3	25/08/2022	Modified version

Table of contents

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 issue and use of electronic signature, authentication and electronic seals certificates offered by the Business Development Agency (hereinafter referred to as the "DEE") as well as the respective commitments and obligations of the various parties involved.

These GTCs apply to any Applicant requesting the electronic certificates offered by the DEE and using the said certificates.

The Holder, respectively the Certificate Manager (CM), 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 DEE.

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 user 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://spe.gouv.mc/entreprises 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 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 Business Certification authority is one of the authorities attached to the TNI.
- **Authorised Representative:** refers to the natural person mandated by the legal representative to manage the company's range of certificates during their life cycle (registration process, including checking the file and the identity of the Holder, renewal and revocation process, etc.). It can be a third party (such as a law firm or an auditor) whose responsibility is engaged through a contractual relationship with the company that empowers him/her to represent it. The legal representative is the default authorised representative.
- **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 DEE's operator in charge of processing certificate application files.
- **Certification Policy or CP**: the CP of Business Certification Authority refers to the document that establishes the principles that apply to the Certification Authority, to legal entities, Legal Representatives, Authorised Representatives and Holders, respectively CMs, involved in the entire lifecycle of a certificate, (which can be consulted at the following address: https://spe.gouv.mc/entreprises)
- 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 Business Certification Authority: 2.16.492.1.1.1.1.4.1.
- **Holder**: refers to the Certificate Holder, a natural person identified in the certificate
- **Registration Process**: refers to the registration process that consists of creating and managing the certificate application file
- **RCI:** The Trade and Industry Registry (RCI) officially lists commercial activities, companies other than civil companies and economic interest groups, and can be consulted at the following link: https://www.rci.gouv.mc/rc/
- **Legal representative:** refers to the person (or persons) legally designated to represent the company. It is the person (or persons) designated in the company's Articles of Association and whose name(s) is (are) entered in the Trade and Industry Registry (RCI).
- **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 seals certificates.

3 CONTACT DETAILS

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

- By post: Direction de l'Expansion Économique - 9 rue du Gabian, MC 98000 MONACO
- By email: esign@gouv.mc.

4 TYPES OF CERTIFICATES AND USES

The types of Certificates issued are as follows:

- Certificates allowing the electronic signature of a natural person representing a legal entity
- Certificates for electronic seal on behalf of legal entities that can be delivered by email (server electronic seal) or on a smart card (smart card seal)
- Authentication Certificates for a natural person representing a legal entity that will allow the natural person to authenticate him/herself in the Administration's online services.

The types of Certificates and uses are described in the CP of the Business Certification Authority (which can be consulted at the following address: https://spe.gouv.mc/entreprises).

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 for Business Certification Authority, which can be consulted at the following address: https://spe.gouv.mc/entreprises.

6 CONDITIONS FOR OBTAINING AND USING THE CERTIFICATE

6.1 APPLICATION FOR CERTIFICATE AND SUPPORTING DOCUMENTS

The registration service offered by the Business Certification Authority is available, by appointment, during the opening hours of the TRADE AND INDUSTRY REGISTRY section.

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

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

Three registration processes are possible:

- Registration process of a Holder, respectively a CM, who undertakes the process for him/herself
- Registration process of Authorised Representatives, which empowers a person to carry out these registration processes for the Registrants, respectively the CMs, of a company.
- Registration process by a Holder, respectively a CM, performed by an Authorised Representative.

Registration requires a prior appointment with a Registration Operator.

The procedures for making an appointment with the DEE, as well as the Certificate application forms in force are available on the following page: https://spe.gouv.mc/entreprises

Copies of the valid identity documents of the Legal Representative and/or Authorised Representative and of the Holder, respectively the CM, must be provided to the DEE in accordance with the conditions in force. The person who visits the DEE in person for the registration process will also have to provide the original his/her ID.

The forms contain the present GTCs and the handwritten signatures of the required persons. They must be dated less than three (3) months before the date of the appointment.

This request is subject to verification and validation by the RA, prior to the issuance of the Electronic Certificate.

The request is traced and kept for ten (10) years.

6.2 ISSUANCE OF THE CERTIFICATE AND ACCEPTANCE

Concerning Certificates for natural persons:

- Issuance of 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 seals 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

At the end of the Certificate delivery process, the Registration Operator gives the Holder, respectively the CM:

- The invoice corresponding to the request

- A document indicating the activation code for each Certificate issued, and the Holder, respectively the CM, is responsible for connecting to the URL that he/she will have received in parallel by email and entering the activation code to retrieve the PIN code corresponding to his/her Certificate within a month of this delivery. Afterwards, he/she will receive, again by email, a revocation code allowing him, if necessary, to cancel his/her Certificate by him/herself.

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.

6.3 USE OF THE CERTIFICATE

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

6.4 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 as follows:

- The Holder or Certificate Manager receives notifications from the certification authority indicating the imminent expiration of the Certificates
- The Holder or Certificate Manager requests an appointment by email at esign@gouv.mc for face-to-face delivery of the new Certificate
- During a renewal, the identification and validation procedure of the renewal request is identical to the initial registration procedure

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.

6.5 REVOCATION

The possible causes of a revocation are described in the CP of the Business Certification Authority (which can be consulted at the following website: https://spe.gouv.mc/entreprises).

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 afteractivation 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 or the Legal 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 Legal Representative or the Authorised Representative may wish, for legitimate reasons, to revoke 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, the Legal Representative or the Authorised Representative, must go in person to the BUSINESS DEVELOPMENT AGENCY 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 revoke 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 Protocol (OCSP), which features a "revoked certificate" response after the certificate's expiry date. Revoked certificates remain in the CRL even after their initial 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, 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 Cardholder, respectively the CM, will assume full responsibility for the consequences of such non-compliance without any recourse against the Business Development Agency.

In the case of a server electronic seal, the RC 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, the CM, or the Authorised Representative changes (e-mail address, etc.), the Holder must inform the CA without delay 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, by the CM, or by the DEE, 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 DEE shall not be liable in any way for the Certificate revocation.

Obligations of the CA:

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

The conditions for ending relations with the Business 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 DEE 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 DEE, 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 DEE intervene, in any way whatsoever, in the contractual relations that may be established between the Holders, respectively the CMs, of the said Certificates.

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

The parties expressly agree that the DEE 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.

10 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, the Authorised Representative and the Legal Representative mentioned in the registration file.

This information includes the following:

Identity/Family status

- Title
- First name
- Surname

Address and contact information

- Professional e-mail address
- Professional phone number (Mobile or Landline)

Education-Diplomas-Professional life

- Company name (of the business)
- RCI Role number in or on behalf of the company
- Company's registered address

Electronic identification data

Data Certificates for natural persons:

- Cn = First name SURNAME
- Serial Number (unique identifier)
- givenName=First name
- surname=SURNAME
- or: organization unit: RCI number
- Title : Role number in or on behalf of the company
- (O : Organization) Corporate name
- C=MC (country)
- Work email address

Certificate data for a legal entity:

- Cn=FQDN, application name, department name, management, entity, etc.
- Serial Number (unique identifier)
- Locality: Monaco (optional)
- State: Monaco (optional)
- or: organization unit: 0206 followed by RCI No. or RC-MC followed by RCI No.
- (O: Organization) Corporate name
- C=MC (country)

Personal answers for unlocking revocation code

4 personal answers out of 7 possible questions (allowing the Holder, respectively the CM, to be identified if he/she has forgotten his/her revocation code)

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 Business Development Agency 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.

11 INTELLECTUAL PROPERTY

The trademarks and/or logos owned by the DEE, 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

In accordance with the provisions of Article 14 of the Act no. 1.165 of 23 December 1993 on personal data protection, amended the information gathered in the context of the issuance of an electronic seal or signature certificate is collected by the State of Monaco (Business Development Agency), which acts as the data controller.

The Business Development Agency operates a personal data processing system for the purpose of "Issuing electronic signature and electronic seal certificates to legal entities".

The processing is part of the Administration's role. It is justified by:

- Compliance with a legal obligation: Sovereign Ordinance No. 11.986 establishing the Business Development Agency
- The realisation of a legitimate interest pursued by the Administration through the development of digital tools and processes in order to offer trusted digital services benefiting from a high level of security and data integrity, in accordance with Act No. 1.383 relating to a Digital Principality, the Digital Economy Act, as amended, as well as its application texts.

The information processed in the context of the provision of an electronic seal or signature certificate to Monegasque companies is intended exclusively for the Administration and the trusted service provider supplying the online service. The data collected will not be communicated for commercial or advertising purposes.

This information is kept only if necessary for the above-mentioned purpose, and in particular:

- Identity, Personal answers for unlocking the revocation code, addresses and contact information, Professional life, any paper documents provided by the applicant: the retention period for this data is ten years (3 years of certificate life + 7 years of additional retention, in accordance with applicable regulations).

- Certificate data: these certificates have a single lifetime of three years.

The information requested in the electronic signature or electronic seal certificates application form for Monegasque companies is mandatory. If the mandatory information is not provided in the contact form, the request for the creation of an electronic signature or electronic seal certificate cannot be taken into account.

In compliance with the legal provisions in force concerning the protection of personal data, the person concerned has a right of access to the processing of his/her personal data; a right to object to their processing, as well as a right of rectification or deletion if the information concerning him/her proves to be inaccurate, incomplete, equivocal, or outdated.

To exercise these rights or for any question related to the processing of your personal information in the context of the application for the creation of an electronic signature or electronic seal certificate, the person concerned may submit a request:

- By clicking here / Going to the gouv.mc website, "Government and Institutions" section / Ministry of Finance and Economy > Business Development Agency > Contact details
- At the following postal address:

Direction de l'Expansion Economique
9, Rue du Gabian
MC 98000 MONACO

To ensure that the response remains confidential and that we are replying only to the person whose data is involved, those submitting requests may be asked to provide proof of their identity, in black and white.

Individuals who have exercised their rights but feel, after contacting the Administration, that their rights have not been respected, can submit a complaint to the Data Protection Authority of Monaco (Commission de Contrôle des Informations Nominatives - CCIN): https://www.ccin.mc/en.

The technical scheme used by the Business Development Agency for the issuance of certificates to companies has been declared to the CCIN and approved.

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 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.