TERMS AND CONDITIONS OF USE FOR THE CONSULAR CERTIFICATES OF THE FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA (FNMT – RCM)

The Applicant declares that, once the Certificate has been downloaded and installed on his/her computer, he/she will acquire the status of Holder and use the Certificate in accordance with the attached conditions and in accordance with the content of the "General Declaration of Trust Services and Electronic Certification Practices" and those of the "Particular Policies and Practices of Consular Certificates" of the FNMT-RCM. expressly declaring that it accepts them in their entirety and that its capacity to contract with this Entity is not limited.

These conditions are an excerpt from the Particular Policies and Practices of Consular Certificates with the basic rules for the issuance of these *Certificates*. The following basic information is made available to the *Applicant* and that, because of space, the duty of information will be satisfied with the *General Declaration of Practices of Trust Services and Electronic Certification* (DGPC) and with the *Particular Policies and Practices of Consular Certificates*, made available in digital format at the previous links.

Type of certificate and limits on use

The Certification Authority issues Electronic Certificates to natural persons with Spanish nationality, of legal age, habitual residents abroad or who are there temporarily, in possession of a Central Consular Identification Number (NICC) and who are not in possession of their National Identity Document (DNI) in force for legal reasons or have never had it.

The type of electronic signature Certificate is:

- Consular Certificate

These certificates can be used for electronic signatures and as an identification mechanism to interact with the General State Administration of the Ministry of Foreign Affairs, European Union and Cooperation, in accordance with the provisions of Royal Decree 991/2024, of 1 October, on the registration of Spanish nationals in the Registration Registers of Consular Offices abroad.

These certificates are issued as an integral part of the identification and electronic signature systems based on qualified electronic certificates admitted by virtue of their inclusion in the lists of trust services in accordance with the technical specifications set out in the Annex I of the Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, as a continuation of the Commission Decision 2009/767/EC of 16 October 2009 (as amended by Commission Decision 2010/425/EU, of 28 July 2010 and the Commission Implementing Decision of 14 October 2013). These lists of trust services contain information concerning the Trust Service Providers that issue qualified certificates to the public, supervised in each Member State, including the FNMT-RCM.

These Electronic Certificates are qualified in compliance with the requirements of Regulation (EU) No. 910/2014, of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market (amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024).

The functionalities and purposes of the Consular Certificates guarantee the authenticity, integrity and confidentiality of the communications in which their Holders participate.

This type of Certificate may not be used for:

- Sign another Certificate, except in cases expressly authorized in advance.
- Sign software or components.
- Generate Time Stamps for Electronic Dating procedures.
- To provide services free of charge or for consideration, except in cases expressly authorized in advance

Validity of Certificates

The Consular Certificates issued by the FNMT – RCM, will have the validity established in its *Particular Policies and Practices of Consular Certificates*, counted from the moment of the issuance of the Certificate, as long as its validity is not extinguished. After this period and if the Certificate is still active, it will expire, and a new one will be necessary to be issued in the event that the Account Holder wishes to continue using the services of the Trust Service Provider.
Consular Certificates may not be used when their validity period expires, when their revocation is requested by the Certificate Holder or when any of the causes for termination of validity established in the General Declaration of Trust Services and Electronic Certification Practices and in the Particular Policies and Practices of Consular Certificates are met.

The validation of the validity status of this type of certificate can be checked through the information and consultation service of the status of the Certificates provided by the FNMT – RCM through the Online Certificate Status Protocol (OCSP), available at the location specified in the certificate itself.

Certificate Renewal

The FNMT-RCM does not contemplate the possibility of renewing Consular Certificates. Once the Certificate has expired, a new Certificate must be requested in order to continue using the services of the Trust Service Provider.

Certificate Revocation

The revocation of Consular Certificates by the FNMT-RCM can be requested by the *Subscriber* or authorized person, during the Certificate's validity period, calling the telephone number provided for that purpose (subject to identification of the Requestor) and posted at FNMT-RCM's website, which shall be operational 24/7, or through the other option described in the Certification Practice Statement. Additionally, the *Certification Authority* and the *Registration Authority* can request a revocation.

In the cases referred to in the *Particular Policies and Practices of Consular Certificates*, the FNMT-RCM may revoke the Subscribers' Certificates. The causes set out in the *Particular Policies and Practices of Consular Certificates* will be valid to revoke a Certificate.

A cause for revocation of a Certificate issued to Natural Persons will also be the request for a new Certificate of the same type issued by the FNMT-RCM.

The revocation of a Certificate will render it invalid before the specified expiration date.

Obligations of the Registry Office

In addition to the obligations and responsibilities of the parties listed in this document and in the General Statement of Trust Services and Electronic Certification Practices, Registry Offices are obliged to:

- To reliably verify the identity and any personal circumstances of the Applicants for the Certificates relevant to their own purpose, using any of the means admitted by law, and in accordance with the provisions of the GCPS and in particular in the *Particular Policies and Practices of Consular Certificates*.
- Keep all the information and documentation related to the Consular Certificates, whose application, renewal or revocation is managed during the period of time established in the current legislation.
- To allow the FNMT-RCM access to the archives and the audit of its procedures in relation to the data obtained in its capacity as Registry Office.
- Inform the FNMT-RCM of any aspect that affects the Certificates issued by said Entity (e.g.: requests for issuance, renewal, etc).
- Comunicar a la FNMT-RCM de forma diligente las solicitudes de expedición de Certificados.
- Diligently verify the causes of revocation that could affect the validity of the Certificates and promptly notify the FNMT-RCM of requests for the revocation of the Certificates.
- Exercise public functions in accordance with the specific legislation applicable to the FNMT-RCM

Obligations of the Certificate holder

The holders of electronic Certificates are required to:

- Know and comply with the conditions of use of the certificates provided for in the conditions of use and in the Certificate Practice Statement and, in particular, the limitations of the certificates' use
- Act diligently with the custody and conservation of signature creation data or any other sensitive information such as keys, certificate request codes, passwords, etc. as well as the certificates resources, which always include the non-disclosure of any of the mentioned data. Request the revocation of the certificate in the event of suspected loss of confidentiality, disclosure or unauthorized use of signature creation data.
- Do not use the *Certificate* when any of the data included in the *Certificate* is inaccurate or incorrect, or there are security reasons that make it advisable, notifying the FNMT-RCM of any modification in the data provided in the certificate application, requesting, when pertinent, the revocation of the same
- Notify the FNMT-RCM of the loss, misplacement or suspicion of the *Certificate*, the Signature Creation Data, the card or support of the Certificate of which you are the Holder, in order to initiate, where appropriate, the procedures for its revocation.

Certificate status verification obligations for third parties

Any third party that reasonably trusts a certificate will have to:

- Ensure that trust in the certificates issued under the certification policy is restricted to the appropriate uses (see *Particular Policies and Practices of Consular Certificates*).
- Verify the validity of the certificate, making sure it has not expired.
- Ensure that the certificate has not been suspended or revoked by accessing information about the current revocation status available at the location specified in the certificate itself.
- Determine that such certificate provides sufficient guarantees for the intended use, as well as checking the limits on use within any Certificate it is verifying.

Disclaimers

The FNMT-RCM will only be answerable for deficiencies in the procedures relating to its activity as a Trust Service Provider, and in accordance with the provisions of these Policies or the Law. In no other event will it be responsible for the actions or losses incurred by holders, subscribers, user entities or third parties involved that are not due to errors attributable to FNMT-RCM in the relevant Certificate issuance and/or management procedures.

The FNMT-RCM will not be answerable in cases of fortuitous event, force majeure, terrorist attack or wildcat strike, or in cases involving actions that constitute crimes or offences that affect its provision infrastructure, except in the event of gross negligence on the entity's part.

The FNMT-RCM will not be answerable to persons whose behavior in the use of the certificates has been negligent; for these purposes, and in any event, negligence will be considered as failure to comply with the provisions of the Certification Practices Statement and, in particular, the provisions in the sections that refer to the parties' obligations and liability.

In any event - this having the status of a penalty clause - the amount that FNMT-RCM must pay by way of damages under legal compulsion to injured third parties or members of the Electronic Community in any public or private field of action, in the absence of specific regulation in contracts or agreements, is limited to a maximum of SIX THOUSAND EUROS (€6,000).

In the event of the termination of the Trust Service Provider's activity, the FNMT-RCM will be governed by the provisions of the current electronic trust services legislation. In any case, it will duly inform the holders of the certificates as well as the users of the services involved in good time and will transfer, with the express consent of the holders, those certificates which remain valid on the effective date of the cessation of activity to another Trust Service Provider that will assume them. If such a transfer is not possible, the validity of the certificates will be extinguished.

The FNMT-RCM registers and archives those significant events that are necessary to verify the activity of this Certification Authority for a period of not less than fifteen (15) years, in accordance with applicable legislation.

In any case, the disclaimers found here are not thoroughly listed, so all legal disclaimers will be met by means of the Trust Services Practices and Electronic Certification General Statement (DGPC) of the FNMT-RCM.

Applicable law, complaints and dispute resolution

The provision of trust services by the FNMT-RCM will be governed by the Laws of the Kingdom of Spain. In general, members of the Electronic Community and Users of FNMT-RCM trust services accept that any litigation, discrepancy, issue or claim resulting from the implementation or interpretation of the Policies and/or Statements of Trust Service and Electronic Certification Practices or related thereto, directly or indirectly, will be resolved in accordance with the provisions of the relevant contracts, general conditions and/or commissions or agreements, in the terms of the entity's By-laws, approved by RD 51/2023 of 31 January (Official State Gazette No. 27 of February 1).

In the event that the contracts, general conditions and/or commissions or agreements do not specify any conflict resolution arrangement, all the parties must submit to the exclusive jurisdiction of the courts of the Spanish State in the city of Madrid.
In addition, mediation or arbitration procedures may be agreed, subject to the approval of the competent bodies of the FNMT-RCM, in accordance with applicable legislation.

The FNMT-RCM will respond to any request, complaint or claim from its customers or third parties that place their trust in its trust services, pursuant to the protocols approved by the Entity.

Licenses and repository, trusted brands and audit
The FNMT-RCM has a lengthy track record in the performance of its industrial activities, as well as the backing of the Central Government as a Public Business Entity attached to the Ministry of Finance and Civil Service. Since the entry into force of Article 81 of Law 66/1997 (30 December) on tax, administrative and social measures and amendments thereto, it has contributed to encouraging the extension of the services for which it is authorised and has obtained the recognition of private business in the electronic certification and open electronic networks sector, achieving a significant position in the provision of trust services.

The FNMT-RCM, as a Trust Service Provider, has a number of accreditations and certificates for its public key infrastructure, of which the following are particularly applicable to certificates of this kind the European Standards:

- ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and
- ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

Consular Certificates are qualified in accordance with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. Their inclusion in the list of trust service providers ("TSL") in Spain may be checked at this link: https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

Trust Service Provider Contact Information
Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda
c/Jorge Juan, 106
28009 Madrid
https://www.sede.fnmt.gob.es/
Contact: ceres@fnmt.es

The FNMT-RCM places at the disposal of the Subscribers, third parties that trust, software suppliers and third parties a communication channel through the electronic venue of the FNMT-RCM (https://www.sede.fnmt.gob.es/) with clear instructions, to allow them to report any matter related to this type of Certificates, regarding a supposed commitment of Private Key, undue use of the Certificates or other types of fraud, compromise, misuse or inappropriate behaviour.

DATA PROTECTION:
Basic information on the personal data collected. This information is made in two layers on the basis of European regulation (articles 13 and 14 of REGULATION (EU) 2016/679 - General Regulation of Data Protection) and Organic Law 3/2018, of December 5, of Protection of Personal Data and guarantee of digital rights.

RESPONSABLE: FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, E.P.E., M.P. (FNMT-RCM).

PURPOSE: Management of the provision of trusted services and other services of the electronic administration and information society, related and foreseen in the purpose of the Entity and in the current regulations. To manage the provision of the above service in all phases of their development and execution.

LEGITIMATION: execution of a contract for the provision of a service to which the interested parties are a party. Compliance with a legal obligation applicable to the data controller. Art. 6.1.c) GDPR: Law 6/2020, of 11 November, regulating certain aspects of electronic trust services and Royal Decree 991/2024, of 1 October, on the registration of persons of Spanish nationality in the Registration Registers of Consular Offices abroad.

DATA COMMUNICATION: Public Administrations, agencies and related or dependent entities, within the scope of article 81 of Law 66/1997, of December 30, 1997, and all other cases contemplated in European and national regulations having the force of Law. Data communications will occur when the certificate serial number is included in the list of revoked certificates. In addition, the use of the certificate enables third parties to access data that you have provided us (name, surname and ID). Communications to the State Security Forces and Corps and judicial authority. No international transfers are made outside the EU.

RIGHTS: You can access, rectify, delete the data and exercise the other rights, as reported in https://www.fnmt.es/politica-privacidad

SOURCE: Unequivocal consent of the interested party. From companies and organizations where services are provided by those affected

SECURITY MEASURES: Esquema Nacional de Seguridad. More information in the lower link.

DATA CATEGORY: Identification data: NIF/DNI, Passport (full content), name and surname, address, telephone number, age, date of birth, email, position, denomination or company name, IP, NICC (Central Consular Identification Number). Personal characteristics data: authenticity public key, private key for cloud signature, certificate serial number, certificate request code. Data on social circumstances: attributes related to the capacity and power of representation. Commercial information data: electronic address (URL).

You may consult additional and detailed information about this treatment in: https://www.fnmt.es/politica-privacidad (DATA PROCESSING Nº 13).