TERMS AND CONDITIONS OF USE FOR INDIVIDUAL CERTIFICATES OF THE SPANISH MINT (FNMT-RCM).

The *Applicant* states that, having downloaded and installed the *Certificate* to his equipment, the Applicant will acquire the status of *Holder* and will use the *Certificate* in accordance with the accompanying terms and conditions and with the Trust Service Practices and Electronic Certification General Statement and the Specific Policies and Practices for Natural Person Certificates of the FNMT-RCM, (https://www.sede.fnmt.gob.es/dpcs/acusuarios) expressly declaring that the Applicant accepts them in full and that the Applicant's capacity to contract with this Entity is not restricted.

These conditions are an extract from the *Specific Policies and Practices for Natural Person Certificates,* with the basic rules for issuing these *Certificates*. The following basic information is made available to the *Applicant*; for reasons of space, the obligation to provide information will be met by means of the *Trust Services Practices and Electronic Certification General Statement* (*DGPC*) and the *Specific Policies and Practices for Natural Person Certificates*, which are made available through the above link in digital format.

Type of certificate and limits on use

The "Users CA" Certification Authority issues electronic certificates exclusively to natural persons who are adults or emancipated minors in possession of a Spanish ID card, tax identity number or alien identity number as an integral part of the electronic identification and signature systems based on qualified electronic certificates admitted by virtue of their inclusion in the trust services lists (TSL) in accordance with the technical specifications set out in the Annex to Commission Decision 2009/767/EC of 16 October 2009 (as amended by Commission Decision 2010/425/EU of 28 July 2010). These TLS contain information on 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23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, which repealed Directive 1999/93/EC.

The functionalities and purposes of the Natural Person Certificates guarantee the authenticity, integrity and confidentiality of communications in which their Holders take part. The Certificate will be issued and signed by the "Users CA", subordinate to the "Root CA" of the FNMT-RCM.

The *Natural Person Certificates* issued by the FNMT-RCM will be valid for a maximum period of four (4) years if the applicant's email is included or it will be valid for a maximum period of three (3) years if the applicant's email is not included, as from the date of issue, provided that they remain in effect. Once the period expires and if the *Certificate* remains active, it will expire and the issuance of a new certificate will be necessary if the *Holder* intends to continue using the services of the *Trust Service Provider.*

The renewal of the *Natural Person Certificates* issued by the FNMT-RCM may be requested by *Holders* thereof provided that at the time of the application they have a *Certificate* in force and their associated *Signature Creation Data* and said application are made in the sixty (60) days prior to its *Expiration.*

Natural Person Certificates may not be used when their validity period expires, when their revocation is requested by the *Holder* of the *Certificate* or if any of the conditions for the termination of their validity are met, as established in the *Trust Services Practices and Electronic Certification General Statement* and in the *Specific Policies and Practices for Natural Person Certificates.*

The length of the key used in the "Users CA" is 2048 bits and in the "Root CA" is 4096 bits.

The validation of the validity status of this type of certificate may be confirmed through the Certificate status information and consultation service provided by the FNMT-RCM through the OCSP protocol, available at the location specified in the certificate itself.

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 on certificate utilisation.
- Act diligently with regard to 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 certificate media, which includes, in any event, 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.
- Duly notify the FNMT-RCM of any modification in the data provided in the certificate application, requesting, when pertinent, the revocation of the same.

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 the Specific Certification Policy and Practices document for natural person certificates of the "Users AC").
- 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.

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 the relevant Certification Policies and Practices. In no event will it be responsible for the actions or losses incurred by applicants, owners, user entities or, as the case may be, 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 behaviour 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 current electronic signature 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 15 years, in accordance with applicable legislation.

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 contracts, general conditions and/or commissions or agreements do not specify any conflict resolution arrangement, all the parties 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.

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:

- Issuance and administration of qualified electronic certificates in accordance with 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". This audit is carried out with the required frequency and by a Compliance Assessment Body accredited for this purpose.

Natural Person 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.* *Quality Management, surveys and opinion polls related to the trust services*
LEGITIMATION	*The consent of the interested party.* *Law 6/2020, of November 11, regulating certain aspects of electronic trust services.*
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 (MAIN PAGE)*
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	*Identifying data, of personal characteristics and social circumstances, as explained in the additional information of the Activities Register of the lower link.*
You may consult additional and detailed information about this treatment in: https://www.fnmt.es/politica-privacidad (DATA PROCESSING Nº 13)	

The interested parties authorize the FNMT-RCM to include the certificate serial number in the list of revoked certificates (data communication) so that it may be viewed by any user, whether or not the user has an electronic certificate, in both the public and private areas. We also inform you, and you agree that the use of the certificate for identification purposes or if you perform an electronic signature, entails the possibility that third parties may access the data you have provided to us that are included in the certificate.
In the following link, you may find information about the Public Registry of Certificate Transparency (CT).