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

The *Applicant* states that, having downloaded and installed the *Public Employee Certificate,* the Applicant will use the *Certificate* in accordance with the accompanying conditions and with the Specific Policies and Practices in relation to the public administrations, government bodies and public entities of the FNMT-RCM (https://www.sede.fnmt.gob.es/dpcs/acap) **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 in relation to the public administrations, government bodies public entities,* 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 in relation to the public administrations, government bodies and public entities*, which are made available through the above link in digital format.

Type of certificate and limits on use

The Public Administration CA issues electronic signature certificates for functionaries and for hired, statutory and authorised personnel working for the Central Government, agency, government body or public entity in the fulfilment of their functions for the certificate subscriber.

The electronic signature certificate for government employees confirms, jointly, the identity of government employees and the certificate subscriber, which is the agency, body or entity of the Public Administrations where said personnel fulfil their functions, provide their services or carry out their activities.

These Utilisation Conditions do not alter or modify the nature, legal regime and competencies of the public administration, body or entity and the personnel where they carry out their public function or activity, and therefore the FNMT-RCM will not be responsible for the actions performed by these employees with the certificates issued in matters that do not originate solely from the organisation and functioning of the FNMT-RCM in the conditions set out in the aforementioned Certification Policies and Practices.

The limits on the use of this kind of certificate result from the competencies and functions of the subscribing Public Administrations acting, where appropriate, through personnel working for them in a signatory capacity, in accordance with their position, work and authorisation conditions.

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 *Public Employee Certificate* guarantee the authenticity, integrity and confidentiality of communications. The *Certificate* will be issued and signed by the "Public Administration CA", subordinate to the "Root CA" of the FNMT-RCM.

The *Public Employee Certificates* issued by the FNMT-RCM will be valid for a maximum period of three (3) years as from the date of issue, provided that they remain in effect. Once the period of validity expires and if the *certificate* remains active, it will expire and the issuance of a new certificate will be necessary if the intention exists to continue using the services of the *Trust Service Provider*.

The *Public Employee Certificates* may not be used when their validity period expires, when their revocation is requested or if any of the other conditions for the termination of their validity are met, as established in the *Trust Service Practices and Electronic Certification General Statement* and in the *Specific Policies and Practices in relation to the public administrations, government bodies and public entities.*

The length of the key used in the "Public Administration 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 Subscribing Entity and/or the person in charge of the Registration Office

The *Certificate Subscriber Entity* and/or the *Person in charge of the Registration Office* are obliged:

- not to register or process applications by personnel that work in an entity different from the entity it represents as Registration Office, notwithstanding the creation of centralised Registration Offices or agreements between branches of the administration for registration purposes;
- to confirm the data of the public employee as user of the Certificate, who will act as the signatory thereof, referring to his identity and the condition of the position, work post, employment or any other data that reflects or characterises the relationship of with the Administration, agency or entity to which the employee

provides his services;

- to request the revocation or suspension of the Certificate of the personnel working for the body represented by the Registration Office when any of the data related to the condition of the position, work post, employment or any other information that reflects or characterises the relationship of the user that signs the Certificate with the body, agency or public entity that subscribes the Certificate and which employs such personnel is inaccurate, incorrect, has changed or needs to be revoked for security reasons;
- in the event that the Certificate is in a card, to download the Certificate and its keys directly on the cryptographic card that is provided to its personnel. not to conserve, in any event, the private keys associated with the Certificates in the Registration Office equipment in accordance with FNMT-RCM guidelines contain in procedures manuals given to the Registration Office, in these Specific Certification Policies and Practices and in the DGPC.

Obligations of public employees

Persons employed by the Public Administrations, as Signatories of the Certificate and its Keys, are obliged:

- not to use the Certificate when any of the data related to the position, work post, employment or any other item is inaccurate or incorrect or does not reflect or characterise their relationship with the body, agency or entity by which they are employed, or if there are security reasons that make this advisable;
- to make appropriate use of the Certificate based on the competencies and authority attributed by the position, work post or employment as public employees;
- notify the Head of the Registration Office of the misplacement, loss or suspicion thereof of the card or Certificate medium of which they are users and custodians, in order to initiate, where appropriate, the revocation proceedings.

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).
- 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, signatories, subscribers, 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 signatories 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 1114/1999 of 25 June (Official State Gazette No. 161 of July 7). 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 certification 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", ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons" and ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons". This audit is carried out with the required frequency and by a Compliance Assessment Body accredited for this purpose.

Electronic signature certificates for persons employed by the public authorities 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://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl

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

DATA PROTECTION.

In accordance with Organic Law 15/1999 (13 December) on the Protection of Personal Data and its enabling regulations, we inform you that the data you provide will be incorporated into a personal data file for which the FNMT-RCM is responsible. Its structure and purpose are as provided in point 5 of the Appendix to order EHA/2357/2008 (30 July) regulating personal data files of the Spanish Mint (Official State Gazette of 7 August) or any legislation by which it is replaced. The information contained in said file is to be used in the provision of electronic, computer or telematic services for the public and private sectors.

Interested parties may exercise their rights of access, rectification, cancellation or opposition before the party responsible for the file (FNMT-RCM) by sending a letter, accompanied by a photocopy of their ID card or an authorisation to consult their identity through the Identification Data Verification System. They may also exercise their rights through the Electronic Register (https://www.sede.fnmt.gob.es/tramites) using the "general purpose form". This entity's registered office is in calle Jorge Juan 106, 28009 - Madrid. The interested parties authorise 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. This is for the purpose of the necessary knowledge by third parties of the purpose and status of the certificate issued or the signature performed, pursuant to Art. 11.2.c) of the Organic Law on Data Protection.