TERMS AND CONDITIONS OF USE OF CENTRALISED ELECTRONIC SIGNATURE CERTIFICATES FOR PUBLIC EMPLOYEES ISSUED BY THE SPANISH MINT (FNMT-RCM).

The *Applicant* states that, once the credentials attesting to his or her identity and the *Electronic Signature Certificate for Public Employees* have been generated, the *Certificate* will be used in accordance with the accompanying terms and conditions and observing the content of the Trust Services Practices and Electronic Certification General Statement **and the** Certification Practices and Policies Statement on Centralised Electronic Signature Certificates for Public Employees **(**https://www.sede.fnmt.gob.es/dpcs/acap**) expressly declaring that he or she accepts them fully and that his or her capacity to make this request is not limited.**

These terms and conditions are extracted from the *Certification Practices and Policies Statement on Centralised Electronic Signature Certificates for Public Employees,* containing the basic regulations for the issuance of these *Certificates*. The *Applicant* is provided with the following basic information and, for reasons of space, the duty of information will be fulfilled by means of the *Trust Services Practices and Electronic Certification General Statement* (*DGPC*) and the *Certification Practices and Policies Statement on Centralised Electronic Signature Certificates for Public Employee*, which are available in digital form through the above link.

Type of certificate and limits on use

The Public Administration CA issues centralised electronic signature certificates to public officials, employees, statutory personnel and authorised personnel working for Public Administrations, government bodies or public-law entities.

These *Certificates* are valid as electronic signature systems pursuant to Law 40/2015 (1 October) on the Public Sector and Law 18/2011 (5 July) on the use of information and communication technologies in the Justice Administration.

The centralised electronic signature *Certificate* for public employees jointly confirms the identity of the government employees and of the certificate subscriber, which is the body or entity of the Public Administration where the employees exercise authority, provide services or perform activities.

The centralised electronic signature *Certificate* for public employees is a certificate type designed to make remote signatures, i.e. the *public and private Keys* are not generated directly in the *Signatory's* Internet browser or in a different device held by the *Signatory*, and the *Certificate* is not downloaded; they are generated and stored in a secure environment owned by the FNMT-RCM. Additionally, the electronic signature is completed in a centralised manner, guaranteeing at all times exclusive control over the signature process by the *Government employees* to whom the *Certificate* has been issued.

These Terms and Conditions of Use do not alter or modify the nature, legal regime or powers of the Administration, Body or Public Entity or of the personnel where the public function or activity is carried out, so the FNMT-RCM will not be liable for actions by these employees using the certificates issued relating to matters that do not arise solely from the FNMT-RCM's organisation and functioning on the terms and conditions stated in the above-mentioned Certification Policies and Practices.

The powers and functions of the Subscriber Public Administration (acting through their personnel as the Signatories of the Certificates) constitute restrictions on the use of this type of Certificates, on the basis of the relevant post, position and, if applicable, authorisation conditions. The FNMT-RCM and the Administration, bodies and public entities may include other additional use scenarios in agreements, regulations or commissions, through the relevant relationship document or in the Issuance Law governing these *Certificates*. These certificates may be used to perform functions pertaining to the post held or in relations with Administrations, bodies and public entities when they allow it under applicable agreements or regulations.

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 centralised electronic signature *Certificate* for public employees allows the authenticity, integrity and confidentiality of communications to be guaranteed. The *Certificate* will be issued and signed by the "Public Administration CA", subordinate to the FNMT-RCM's "Root CA".

The *centralised electronic signature Certificates for public employees* issued by the FNMT-RCM will be valid for a maximum of three (3) years as from the moment the *Certificate* is issued, provided validity is not terminated. 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 *centralised electronic signature Certificate for public employees* may not be used once its validity period has expired, revocation is requested or due to any of the causes for termination of validity stipulated in the *Trust Services Practices and Electronic Certification General Statement* and in the *Specific Policies and Practices relating to Public Administrations, bodies and public-law entities.*

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

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 Registration Offices of the FNMT Registration Authority are obligated to:

- Verify irrefutably the identity and any personal circumstances of the *Applicants* of the *Certificates* relevant to the purposes for which they are intended, using any of the means permitted by law and in accordance with the *Certification Practices and Policies Statement*.
- Inform Certificate users of their adequate use, pursuant to these terms and conditions, the Certification Practices and Policies Statements and applicable legislation.
- Preserve for the period of time stipulated in prevailing legislation all information and documentation relating to Certificates the application, renewal or revocation of which is managed.
- Allow the FNMT-RCM to access the archives and audit their procedures in relation to the data obtained as a Registration Office.
- Report to the FNMT-RCM any aspect that may affect the Certificates issued by the Entity (e.g. applications for issuance, renewal…).
- Diligently report Certificate issuance requests to the FNMT-RCM.
- As regards the expiration of Certificates:
    - Diligently check the causes for revocation that could affect the validity of the Certificates.
    - Diligently report Certificate revocation requests to the FNMT-RCM.
- As regards personal data protection, the provisions of the relevant section of the Certification Practices and Policies Statement will be applicable.
- The Registration Offices, through the personnel assigned to the service as employees or public officials, must carry out public functions pursuant to the specific legislation applicable to the FNMT-RCM.

Obligations of public employees

The natural person associated with the *Certificate*, who acts as the *Signatory,* must comply with the security standards related to the custody and use of the PIN, as confidential, personal and non-transferable information that guarantees access to his or her *Private keys*. Accordingly, the *Holder* must observe the following cautions relating to the PIN:

- Protect its confidentiality, avoiding disclosure to other persons.
- Memorise it and not write it down in any physical or electronic document.
- Change it as soon as he suspects that it may be known to another person.
- Notify the FNMT-RCM of any possible loss of control over his Private key in order to revoke the Centralised Signature Certificate and associated Keys.
- Refrain from choosing a PIN that may be easily deduced from his or her personal data or is predictable (date of birth, telephone number, series of consecutive numbers, repetitions of the same character, etc.).
- Follow the FNMT-RCM's security policy regarding PIN composition, frequency of changes, etc.

Certificate status verification obligations for third parties

The rest of the Electronic Community, User entities and third parties will regulate their relations with the FNMT-RCM through the DGPC and, if applicable, through the Certification Practices and Policies Statement, all without prejudice to the provisions of electronic signature legislation and other applicable laws.

The members of the Electronic Community, User entities and third parties placing their trust in the Certificates and in the Electronic signatures generated using them must be familiar with the Certification Practices and Policies Statement (as a document published in the FNMT-RCM's electronic site) and fulfil the following obligations, holding the Trust Service Provider harmless from any liability if they are not observed:

- Verify, before placing their trust in the Certificates, the advanced Electronic signature or Electronic stamp of the Trust Service Provider that issued the Certificate.
- Check that the Signatory's Certificate is still valid.
- Verify the status of the Certificates in the Certification Chain by consulting the FNMT-RCM's Certificate validity status information and consultation service.
- Check the restrictions on use applicable to the Certificate verified.
- Ascertain the terms and conditions of use of the Certificate pursuant to the Certification Practices and Policies Statement.
- Notify the FNMT-RCM or any Registration Office of any anomaly or information relating to the Certificate that might be regarded as a cause for revocation, providing all evidence available.

Disclaimers

The FNMT-RCM will only be answerable for the correct personal identification of the Applicant and future Holder, and for including these data in a Certificate. In order for the guarantees, obligations and responsibilities to be applicable, the event must have taken place within the scope of the Electronic Community.

The FNMT-RCM will only be answerable for weaknesses in the procedures pertaining to its own activities as a Trust Service Provider and in accordance with these Certification Policies or the Law. It will not in any circumstances be liable for actions or losses that may be incurred by Holders, Subscribers, User entities or third parties which are not due to errors attributable to the FNMT-RCM in the above-mentioned Certificate issuance and/or management procedures.

The FNMT-RCM will not be liable for force majeure events, terrorist attacks, wildcat strikes or actions constituting offences or misdemeanours that affect its facilities in which the services are provided, unless the entity is guilty of serious negligence. In any event, the FNMT-RCM may include disclaimers in the relevant contracts and/or agreements.

In any case, the amount of damages that the FNMT-RCM would be required to pay to affected third parties and/or members of the Electronic community as a result of a court order, in the absence of specific provisions of contracts or agreements, is limited to a maximum of SIX THOUSAND EUROS (€6,000).

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

The FNMT-RCM will not be liable for any software that it has not provided directly. Nonetheless, the FNMT-RCM will put in place adequate measures to protect its systems against Malicious software (Malware) and will diligently keep them up to date to cooperate with users in the avoidance of the damage that such software may cause.

The FNMT-RCM does not guarantee the cryptographic algorithms and will not be liable for damage caused by successful external attacks on the cryptographic algorithms used, provided it acted with due diligence based on the current state of technology and in accordance with this *Certification Practices and Policies Statement* and the Law.

Applicable Law, Complaints and Dispute Resolution

The provision of trust services by the FNMT-RCM will be governed by the laws of Spain. In general, the members of the Electronic Community and Users of the FNMT-RCM's trust services accept that any lawsuit, discrepancy, matter or claim arising from the enforcement or interpretation of the Trust Service and Electronic Certification Practices Policies and/or Declarations or related to them directly or indirectly will be resolved in accordance with the provisions of the relevant contracts, general terms and conditions and/or commissions or agreements, in the terms stated in the entity's Statute introduced under RD 1114/1999 (25 June) (Official State Gazette no. 161 of 7 July). In the event that contracts, general

terms and 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.

Qualification 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 of 30th 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" 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.

Electronic signature certificates for public employees 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

PROTECCIÓN DE DATOS.

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. Once your relationship with the FNMT-RCM is over, we will keep your information blocked for the exercise of rights.*
LEGITIMATION	*The legal basis for the treatment of your data is the need to manage them to perform the service as a trusted third party*
RECIPIENTS	*Your serial number of the certificate will be communicated to third parties in order that they can verify its validity and the data included in the certificate when it is used. No international transfers are made outside the EU.*
RIGHTS	*You can access, rectify, delete the data and exercise the other rights, as reported in http://www.fnmt.es/rgpd (MAIN PAGE)*
SOURCE	*Unequivocal consent of the interested party. From organizations where services are provided by those affected (representatives, representatives or contacts)*
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:

http://www.fnmt.es/rgpd (TRATAMIENTO Nº 15)

Los interesados podrán ejercitar los derechos de acceso, rectificación, cancelación y, en su caso, oposición ante la FNMT-RCM remitiendo un escrito, adjuntando una fotocopia de su DNI o autorizándonos la consulta al Sistema de Verificación de Datos de Identidad. También puede ejercitar sus derechos a través del Registro Electrónico (https://www.sede.fnmt.gob.es/tramites) utilizando el "Formulario de propósito general". El domicilio de esta Entidad es calle Jorge Juan nº 106, 28009 - Madrid. Los interesados autorizan a la FNMT-RCM a incluir el número de serie del certificado en la lista de certificados revocados (comunicación de datos) para que sea visualizado por cualquier usuario, aunque no disponga de un certificado electrónico, tanto en el ámbito público como privado. Además, le informamos y usted consiente, que el uso del certificado a efectos de identificación o si realiza una firma electrónica, posibilita que los terceros puedan acceder a los datos que nos ha proporcionado incluidos en el certificado.

Información sobre Registros públicos de Certificate Transparency (CT).