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

The *Applicant* states that, having downloaded and installed the *Component Certificate*, the Applicant will use the *Certificate* in accordance with the accompanying conditions and with the Trust Service Practices and Electronic Certification General Statement and the Specific Policies and Practices for component certificates of the FNMT-RCM, (https://www.sede.fnmt.gob.es/dpcs/accomponentes) 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 component certificates of the FNMT- RCM,* 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 component certificates of the FNMT-RCM*, which are made available through the above link in digital format.

Type of certificate and limits on use

The "Components CA" Certification Authority issues the following types of electronic certificate, with their specific scope of use:

• Standard SSL web site Certificate: Allows secure communications using the SSL/TSL protocol. This type of Certificate guarantees the identity of the domain where a web is located. This certificate will be valid for a maximum period of two (2) years as from the date of issue, provided that it remains in effect.

• SSL Multidomain web site Certificate (SAN/UCC): Guarantees the security of a set of domains independent of each other. This certificate will be valid for a maximum period of two (2) years as from the date of issue, provided that it remains in effect.

• Wildcard web site Certificate: The wildcard certificate identifies all subdomains associated with a specific domain without the need to acquire and manage multiple electronic certificates. This certificate will be valid for a maximum period of two (2) years as from the date of issue, provided that it remains in effect.

• Entity Electronic Seal: Used for the automation of signature and authentication processes between computer components. In addition, the user is allowed to choose the extended use of the Certificate's keys (client authentication, e-mail protection). This certificate will be valid for a maximum period of three (3) years as from the date of issue, provided that it remains in effect.

Once the period of validity of the certificates terminates and if the certificate remains active, it will expire and the issuance of a new certificate will be necessary if the user wishes to continue using the services of the Trust Service Provider. Component 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 for Component Certificates of the FNMT-RCM.

These electronic certificates are issued 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 length of the key used in the "Components 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 Subscriber Entity and of the certificate applicant

- Not to use the *Certificate* outside the limits specified in the present specific *Certification Policy and Practices*.

- Not to use the *Certificate* in the event that the *Trust Service Provider* which issued the certificate in question has ceased its activity as a *Certificate* Issuer, particularly in cases where the provider's *Signature Creation Data* may be compromised, and this has been communicated.
- Provide truthful information in *Certificate* application and keep it updated, the contracts being signed by persons with sufficient capacity.
- Not to request for the *Subject* of the certificate any distinctive signs, denominations or industrial or intellectual property rights of which it is not the owner or licensee, or in relation to which it does not have demonstrable authorisation for the use thereof.
- Act diligently with regard to the custody and maintenance of the *Signature Creation Data* or any other sensitive information such as *Passwords*, *Certificate* activation codes, access words,personal identification numbers, etc., and to the media of the *Certificates,* which includes, in all cases, the non-disclosure of any of the above-mentioned data.
- Know and comply with the conditions of use of the *Certificates* provided for in the conditions of use and in the *Certification Practices Statement* and in particular, the limitations on the use of *Certificates.*
- Know and comply with any changes that occur in the *Certification Practices Statement*.
- Request the revocation of the corresponding *Certificate* in accordance with the procedure described in this document, diligently notifying the FNMT-RCM of the circumstances of the revocation or suspected loss of *Confidentiality*, the disclosure, modification or unauthorised use of the *Signature Creation Data*.
- Review the information contained in the *Certificate* and notify the FNMT-RCM of any errors or inaccuracies.
- Verify, before trusting the *Certificates,* the *recognised electronic signature* of the *Trust Services Provider* issuing the *Certificate.*
- Duly notify the FNMT-RCM of any changes in the data provided in the application for the *Certificate*, requesting, when pertinent, the revocation of the same.
- Return or destroy the *Certificate* when required by the FNMT-RCM, and not use it for electronic signing or identification purposes when the *Certificate* expires or is revoked.

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 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.

Return policy

In a context of good business practices, the FNMT-RCM has adopted a policy for returning issued certificates that allows refunds to be requested within the established termination period, accepting that this will lead to the automatic revocation of the certificate.

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:

- Entity Electronic Seal, standard SSL, multidomain SSL, and wildcard web site certificates: Issued in accordance with the European standard ETSI EN 319 411-1 "Policy and Security Requirements for Trust Service Providers issuing certificates- General Requirements"
- Entity Electronic Seals 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 319 412-3 "Certificate profile for certificates issued to legal persons".
- Standard SSL: issuance and administration of qualified electronic certificates in accordance with the European standards ETSI with ETSI EN ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI EN 319 412-4 "Certificate profile for web site certificates".

This audit is carried out with the required frequency by a Compliance Assessment Body accredited for this purpose.

Entity Electronic Seals 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.aspxTrust 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. 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)

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 FNMTRCM 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).