

CORPME TRUST SERVICE PROVIDER

QUALIFIED CERTIFICATE OF LOCAL ADMINISTRATION USE LICENSE

In, 20.....

Mr/Mrs/Ms/Miss,
with DNI/NIF/Passport/NIE nº, e-mail, phone number
....., representing the local administration,
..... with NIF nº,
from the province and the local unit,
with the administrative position

REQUEST: The holder states that he/she has generated a private key in a secure cryptographic device and he/she requests CORPME the issuance of a **Qualified Certificate of Local Administration** and he/she undertakes to use it in accordance with the CORPME¹ Certification Practice Statement and the Certification Policy for external Certifications. Furthermore he/she requests the revocation of all **Qualified Certificates of Local Administration** in its name existing prior to the issuance of the certificate object of this document.

ACCEPTANCE The holder declares that he/she has received the certificate, accepting that each digital signature created using the private key corresponding to the certified public key is his/her electronic signature and he/she knows that the use of the certified private certificate is personal and non-transferable, assuming the responsibility for the misuse of it as well as the potential related damages. He/she also accepts the corresponding usage limitations and states he/she will not use the private key to issue public key certificates or revoked certificate lists.

Mr/Mrs/Ms/Miss,
Processing Unit Responsible

CERTIFICATION: It certifies that, in its presence, the holder has generated in a secure cryptographic device a private key and has received from CORPME the corresponding **Qualified Certificate of local Administration**, all in accordance with the provisions of the Certification Policy for External Certificates and In the CORPME Certification Practice Statement.

Signed: The Holder

Signed: Processing Unit Responsible

Basic information about Data Protection:

Responsible for the treatment: CORPME.

Purpose of the treatment: Management of the request made by the user, execution of the agreement signed and / or provision of the electronic signature service; based on what is indicated in the additional information that reference later.

Legitimation: Contract and / or provision of the electronic signature service.

Recipients: It is not foreseen the communication of your personal data except when necessary to comply with legal obligations or necessary for the execution of the contract or agreement subscribed in your case.

Rights: Access, rectify and delete data, as well as other rights, as explained in the additional information.

Additional information: You can consult additional and detailed information on data protection in the data protection conditions of this document.

¹ The Certification Practices Statement and the Certification Policy can be consulted at the address <http://pki.registradores.org/normativa/index.htm>

CERTIFICATION TERMS AND CONDITIONS AND DISCLOSURE STATEMENT

This document constitutes an extract of the rights and obligations contained in the Certification Practice Statement (hereinafter, CPS) of the Colegio de Registradores de la Propiedad y Mercantiles de España CORPME, The Public Corporation of Land and Business Registers of Spain (hereinafter CORPME) and applies to the **Qualified Certificates of Local Administration**. These Terms and Conditions develop the published CPS and the Certification Policies (hereinafter, CPs).

The legal effects of a certificate, as well as the related rights and obligation, will be interpreted in all cases according to the current legislation, the CPS and the CP of External Certificates in the version allocated in the following URL: <http://pki.registradores.org/normativa/index.htm>.

Before requesting a certificate or making use of it as a mechanism for checking electronic signatures, it is recommended to read these Terms and Conditions, in order to assess the trust offered by it. Ignorance of these Terms and Conditions may not be claimed to exempt from the responsibilities or to require them elsewhere.

1. *Trust service provider contact Information*

Colegio de Registradores de la Propiedad y Mercantiles de España.

Prestador del Servicio de Certificación del CORPME.

C/ DIEGO DE LEON, 21.

28006-MADRID

Teléfono: 902181442 / 912701699

Email: psc@registradores.org

Web: <http://pki.registradores.org/normativa/index.htm>

2. *Type of certificate, validation and use procedures*

Qualified Certificates of Local Administration are certificates of non-transferable use certifying the holder identity, as well as its condition of staff assigned to local administration. They are issued for the exclusive use in the scope of their activity, in the relation with the Spanish Registers and with other Public Administrations. Their main purpose is the signing of documents, guaranteeing the authenticity of the issuer, non-repudiation of origin and integrity of the content. They can also be used to ensure the holder's authentication to systems that require access control and e-mail signature.

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.

The **Qualified Certificates of Local Administration** are governed by the certification policies of ETSI EN 319 411-2, regarding QCP-n-qscd.

These certificates are issued under the policy with OID 1.3.6.1.4.1.17276.0.2.4.2 detailed in the CP for External Certificates.

3. *Limits of use*

Qualified Certificates of Local Administration must not be used when their validity period expires, when their revocation is requested or when any of the causes of extinction of the validity established in the CPS and in the CP of External Certificates are fulfilled.

Certificate users can check the validity of the certificate in the Certification Validation Service, through the address where the OCSP is available.

A directory containing the Revoked Certificate Lists (hereinafter CRLs), signed by the Trust Service Provider (TSP), is also published and updated each time a certificate is revoked.

Electronic signatures received outside the validity period of the certificate will not be considered valid, except when it is established that the signature was made within it, by means of a time stamp of the Registers or another time stamp system recognized by the CORPME TSP.

Before validating an electronic signature, it will be necessary to verify that the certificate supporting it has not been revoked through the Certificate Validation Service, through the OCSP, or through the directory containing the CRLs.

The certificates are electronically signed by the CORPME TSP with the private key corresponding to the class of the external certificates and are issued in accordance with the International Telecommunication Union standard number X-509, version 3.

The length of the certified keys is 2048 bits and its validity period is two (2) years.

The use licenses, revocation requests, credential certifications for certifiable attributes, and in general, any signed documents related to rights and obligations for the participants in the CORPME TSP, as well as the associated audit records, shall be stored for a minimum period of fifteen (15) years.

The CORPME will use different systems to issue and revoke certificates, providing high availability to the service. In addition, the certificate status information service, in its two variants (CRLs and OCSPs), is available 24

hours every day of the year, both for third parties who trust and for certificates holders or other parts require them.

4. Renewal

From CORPME systems the holder will be notified through the provided email the future expiration of the certificates, at least two (2) months before the date of expiration, indicating the steps to be followed to obtain a new certificate, in accordance with the procedure established in the CPS.

5. Revocation

The revocation of a certificate implies its total loss of validity and the exemption of responsibility of the TSP for any damage caused as a result of the use of the revoked certificate after its revocation.

The revocation will have effects against the applicant from the moment he submits the corresponding request to the Processing Unit and, as against third parties, since it is published in the Directory of Revocation Lists. It shall be the duty of the holder to check if the revocation of the certificate has been published in the Directory of Revocation Lists http://pki.registradores.org/crls/crl_ext_psc_corpme.crl.

In order to request a certificate revocation in person, the holder must appear before the Processing Unit where it was issued or, in case of emergency, in any other CORPME Processing Unit. The Processing Unit Responsible will verify the identity of the applicant and proceed to the revocation of the certificate, keeping the request for revocation signed by both for fifteen (15) years.

In addition, the revocation of the certificates may be requested signing an electronic application, as stated in the CORPME CPS. The Central Processing Unit will proceed to the revocation and it will notify the holder the confirmation of the revocation status. The web address to access this online revocation service is <https://pki.registradores.org/rauserrevocserver/>.

The Governance Board may order the Central Processing Unit to revoke a certificate, without prejudice to the responsibilities in which it may incur. The order will indicate the period within which the revocation must proceed. The Processing Unit will immediately notify the holder by email and will proceed with the revocation in that very moment.

The services provided make available to the user a Certificate Revocation List (CRL) service, based on the provisions of ITU-T X.509 and an Online Certificate Status Verification (OCSP) service, based on the established in IETF RFC 6960. Both services complement each other and are configured in such a way that they comply with the ETSI EN 319 411-2 standard. Revocation information is available online 24 hours a day, every day of the year, both for trusting third parties and for certificate holders or other parties that require them. The information about the revocation will be kept until the expiration date of the certificate. In case of compromise of the private key concerning the CA of the certificate or in case of termination of CA services, CORPME will make the information available both to trusting third parties and to certificate holders or other parties that require it. revocation until all concerned certificates have expired.

6. Obligations of the certificate holder

The **Qualified Certificate of Local Administration** must be used in accordance with its purposes, aligned with what is established in Spanish legislation, in the CPS and in the published CPs.

In particular, the holder obligations are:

- To provide the Processing Units with accurate, complete and trusted information regarding the data requested to carry out the registration process.
- To inform the CORPME PKI (Public Key Infrastructure) managers with any changes of this information.
- To know, accept and sign the certificate use license.
- To use the certificate exclusively for the uses specified in these Terms and Conditions and in the certificate itself, and only within its validity period.
- To protect and store the private cryptographic keys as confidential and un-accessible from unauthorized third parties, taking the necessary security measures to preserve them.
- To maintain secrecy about the password protecting the private key, and the revocation code used to revoke the certificate.
- To immediately notify the corresponding Processing Unit the loss or disclosure of the private key, or any situation that may affect the certificate validity, pursuant the procedures provided for in the CPS and CPs.
- To do not use the private key if the Certification Authority (CA) or the Registration Authority (in advance, RA) have suspended or revoked it or after the expiration of the certificate period of validity.
- Refrain from using the private key of the certificate from the moment the compromise is notified or warned
- To destroy the certificate when required by the CA, by virtue of the right of ownership that in any case retains on it and when the certificate expires or is revoked.

- To do not monitor, manipulate or perform "reverse engineering" on the technical implementation (hardware and software) of the certification services, without CA prior written permission.
- To do not transfer or delegate responsibilities over a certificate assigned to a third-party.
- To install the certificate only on servers accessible to the enumerated subjectAltName (s) in the certificate profile.
- To respond the CA's instructions regarding certificate compromise or certificate misuse within a specified period of time.
- To recognize and accept the CA right to immediately revoke a certificate if the applicant violates the Terms and Conditions or if it is discovered that the certificate is being used in criminal activities, such as fraud or distribution of malware.
- Create all digital signatures using the QSCD in which the public and private keys of the certificate are generated and which is delivered to the subscriber at the time of issuance

7. Third parties' obligations verification of status certificates

Any third party relying in a certificate must:

- Verifying, before trusting in a certificate, the validity and that it has not been revoked. To this end, it must verify the status and the validity period by any of the available means: consultation of the CRLs or online status consultation by means of OCSP before accepting any communication or document signed digitally with a Certificates issued by the CORPME.
- Limit the certificate use to the allowed purposes, in accordance with the extensions of the certificates and the corresponding CP.
- Assume the responsibility in the correct verification of electronic signatures.
- Assume the responsibility in verifying the trusted certificate validity, revocation or suspension and validity period.
- Know the guarantees and responsibilities derived from the acceptance of the trusted certificates and assume their obligations.

8. Limitations of liability

The TSP will not be responsible, in any case, for the use of the certificates, nor for the errors, neither for the interpretation committed by those who validate a signature. In particular, the TSP shall have no liability for:

- Damages, direct or indirect, caused by the use of certificates and certified keys in not allowed uses or outside the validity period, as well as for the loss or disclosure of the holder's private key.
- The content of the documents signed with a digital signature based on a certificate issued by him/her or the information contained in a server certified by him/her.
- Failures or errors due to the computer equipment, browsers or applications used by the owner or by third parties.

9. Applicable agreements, Certification Policies and Certification Practice Statement

The CPS and CP of External Certificates, published at <http://pki.registradores.org/normativa/index.htm>, include the public information of the Terms and Conditions and characteristics of the certification services provided by the CORPME as TSP, containing the obligations and procedures in relation to the issuance of **Qualified Certificates of local Administration**.

The activities that the CORPME may subcontract to carry out its activity as TSP are carried out contractually according to the CPS. In these cases, the access to the information owned by the CORPME follows the protocol defined in the Security Policy, in terms of the identification of risks, establishment of security controls to protect access formalizing confidentiality agreements and, if applicable, processing of personal data in compliance with current regulations.

10. Privacy Policy

In accordance with the General Data Protection Regulation (REGULATION UE 2016/679), the user and owner of the data is informed that the person in charge of the processing of their personal data is the COLLEGE OF REGISTRARS OF THE PROPERTY AND COMMERCIALS OF SPAIN (in forward, "CORPME"), with CIF: Q-2863012-G and Colegial Headquarters in Calle Diego de León, 21, 28006 in Madrid. The processing of your personal data will be done by the CORPME for the following purposes based on the type of document subscribed by the user:

- User Licenses: to process the presented request and the corresponding billing.
- Revocation requests: to process the certificate revocation request.
- Functions delegation: to process requests and to issue digital certificates according to the CORPME's Certification Practice Statement as Trusted Service Provider.

- Responsible Statement of Trusted Roles: to process the statement of their responsibility as Trusted Role.
- Registrar's Statement of Registry's employees: to process the registrar's statement and to issue the digital certificate.

The legitimizing basis that enables the processing of your data is the execution of the service or contract requested by the interested party or compliance with the agreement signed in his case.

Likewise, the user is informed that their data will be transferred only to comply with the legally established obligations or be necessary for the execution of the contract or agreement subscribed in their case.

The personal data requested in the form are essential for the management of the request made by the user, the execution of the agreement subscribed and / or provision of the electronic signature service, so that the refusal to supply them will imply the impossibility of its realization. The user will be responsible for the accuracy and truthfulness of the data supplied.

No personal data will be made available to third parties except in the legally foreseen scenarios or if it is needed to the agreement execution, or when required to do so by mandate of the authority competent in accordance with law or as a necessary requirement for the subscription of the requested contract.

We inform you of the existence of the right to request the data controller to access the personal data relating to the interested party, and its rectification or suppression, or the limitation of its treatment, or to oppose the treatment, as well as the right to portability of the data. Similarly, the user can claim before the Spanish Agency for Data Protection (AEPD) www.agpd.es.

You can obtain more information about the processing of personal data made by CORPME in the data protection policies available on the web: www.registradores.org.

The maximum period of conservation of the data will be 15 years. In any case, the CORPME may retain the data of the holders for a longer time in those cases where it is necessary due to the existence of responsibilities derived from the service provision.

Those interested can contact the CORPME Data Protection Delegate through email dpo@corpme.es.

11. Return Policy

Not applicable.

12. Applicable Law, claims and dispute resolution

The operations of the CORPME TSP, as well as the CPS and the CP's for each type of certificate, will be subject to the applicable regulations, specially:

- 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Ley 39/2015, of 1 October, about Common Administrative Procedure of the Public Administration.

All claims between users and the CORPME shall be communicated by the disputing party to the CORPME, in order to attempt to resolve it.

For the resolution of any dispute regarding the provision of certification services, the parties are submitted to the Spanish courts and tribunals, regardless of where the certificates were issued.

13. Licensing and repository, trusted brands and audit

The CORPME, as TSP, maintains several accreditations and certifications for the public key infrastructure, especially remarkable:

- Issuance and administration of qualified electronic certificates in accordance with 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".

The inclusion of the qualified certificates issued by CORPME in the list of trust service providers (TSL) of Spain and the European Union can be verified, through the following links:

<https://eidass.ec.europa.eu/efda/tl-browser/#/screen/tl/ES/12>

Likewise, CORPME is registered as a qualified provider with the Ministerio de Asuntos Económicos y Transformación Digital:

<https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx>

<https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx>

The above information sources, as defined by RFC 5280, are established as the Trust Anchor, which is the end point of a certificate validation process. Trust Anchors guarantee the digital identity of the service identified in the trust service entries as defined in ETSI TS 119 61.

In accordance with the provisions of EU Regulation No. 910/2014, CORPME will carry out biennial audits in accordance with said Regulation.

Signed.: The Holder

Version: July 2023