Registradores DE ESPAÑA

CORPME INTERNAL CERTIFICATION POLICIES

Trust Service Provider

Information Systems Service
August 23th, 2017

COLEGIO DE REGISTRADORES DE ESPAÑA
Diego de León, 21 - 28006 Madrid
Tel.: +34 91 270 16 99 - Fax: +34 91 562 67 37

DOCUMENTAL CONTROL

DOCUMENT / FILE	
Title: CORPME Internal Certification Policies	File/s name: REG-PKI-DPC02v.1.2.0 CORPME Internal Certification Policies.pdf
Code: REG-PKI-DPC02	Logical Support: MS-DOCX y PDF
Date: 23/08/2017	Physical location: http://pki.registradores.org/normativa/index.htm
Version: 1.2.0	

CHANGE RETENTION		
Version	**Date**	**Reason for change**
1.0.0	20/06/2016	Document approval
1.0.1	19/09/2016	Modification LFE/2016/0071
1.0.2	27/10/2016	Modification (2) LFE/2016/0071
1.0.3	23/11/2016	Modification (3) LFE/2016/0071
1.0.4	23/12/2016	Modification (4) LFE/2016/0071
1.0.5	29/05/2017	Adaptation to eIDAS Regulation
1.1.0	26/06/2017	Adaptation as a result of audit according to ETSI standards
1.2.0	23/08/2017	Minor corrections

INDEX

1 INTRODUCTION

1.1 Overview

The Public Corporation of Land and Business Registers of Spain, Colegio de Registradores de la Propiedad y Mercantiles de España (hereinafter CORPME), Public Law Corporation attached to Justice Ministry Registers and Notary General Directorate, is constituted as Electronic Signature Certification Services Provider under of the mandate made by the Legislator in the additional provision 26 of Act 24/2001, of December 27th, on Fiscal, Administrative and Social Order Measures. It was born with the purpose of offering the necessary mechanisms and systems to guarantee telematics communications security in which the Registrars, the Public Administrations, the professionals that deal with the Registers and the citizens in general take part.

The TSP CORPME internal regulations are the basic Certification Service standard, which establishes its nature, structure and organization, as well as the criteria and procedures that the Service undertakes to follow in the exercise of its activity, request of the certificates and generation of the keys, until the later emission, distribution, use, revocation and renewal of the same ones.

The Certification Practice Statement (hereinafter CPS), issued in accordance with Article 19, Law 59/2003 of Electronic Signature, defines and documents a general regulatory framework, according to which the CORPME Certification Service Provider activity in relation to digital certificate life cycle application, emission and management processes including certificates validity, revocation and renewal verification procedures.

The standards and regulations that apply and comply with this document are:

- **RFC 3647**: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*
- **ETSI TS 102 042**: *Policy requirements for certification authorities issuing public key certificates.*
- **ETSI TS 101 456**: *Policy requirements for certification authorities issuing qualified certificates.*
- **ETSI TS 102 023***: Policy requirements for time-stamping authorities.*
- **ETSI TS 101 862***: Qualified Certificate profile.*
- **ETSI TS 101 861***: Time stamping profile.*
- **ETSI EN 319 401***: General Policy Requirements for Trust Service Providers.*
- **ETSI EN 319 411-1***: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.*
- **ETSI EN 319 411-2***: Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates.*
- **ETSI EN 319 412-1***: Certificate Profiles. Overview and common data structures.*
- **ETSI EN 319 412-2***: Certificate Profiles. Certificate profile for certificates issued to natural persons.*
- **ETSI EN 319 412-5***: Certificate Profiles. QCStatements.*
- **ETSI EN 319 421***: Policy and security requirements for Trust Service Providers issuing Time-Stamps.*
- **CA/Browser Forum:** *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.*

The Certification Policies (hereinafter CP's) applicable to each class of certificate complement the general provisions in the CPS. In case of conflict or contradiction between the provisions of the CPS and the aforementioned Policies, the precepts in the latter will prevail.

The CP's also define the scope of potential holders of the certificates, as well as the intended uses of the certificates issued by CORPME.

Qualified certificates included in the respective CP's, comply with EU Qualified Certificates and require the use of a Secure Signature Creation Device.

CORPME's activity will be carried out in full compliance with the requirements of Law 24/2001, of December 27, Law 59/2003 of Electronic Signature, of December 20, all of state level; To EU Regulation 910/2014 on Electronic Identification and Trusted Services, and the PSC Rules of Procedure.

This CP assumes that the reader is familiar with the concepts of PKI, certificate and Electronic Signature; otherwise, it is recommended that the reader is trained in the knowledge of the above concepts before continuing with the reading of this document.

1.2 Document Name and Identification

This document is called *CORPME INTERNAL CERTIFICATION POLICIES.*

Document Identification:

Document's name	CORPME Internal Certification Policies
Document's version	1.3.0
Document's status	Version
Date of Issue	23/08/2017
Date of expiration	No applicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.1.0.1.1.0
CP location	http://pki.registradores.org/normativa/index.htm
Related CPS	Certification Practice Statement

1.3 Participants in the Public Key Infrastructure (PKI) of the Trust Service Provider of the CORPME

1.3.1 Trust Service Provider (TSP)

The Trust Service provider is the entity responsible for the issuance, under the hierarchy of its root certificate, of the digital certificates for final entities, and for the life cycle management of the digital certificates.

The CORPME Trust Service Provider legal information and identifying data is available at **http://pki.registradores.org/normativa/index.htm.** A printed copy of such documentation may also be requested by any interested party at the following address:

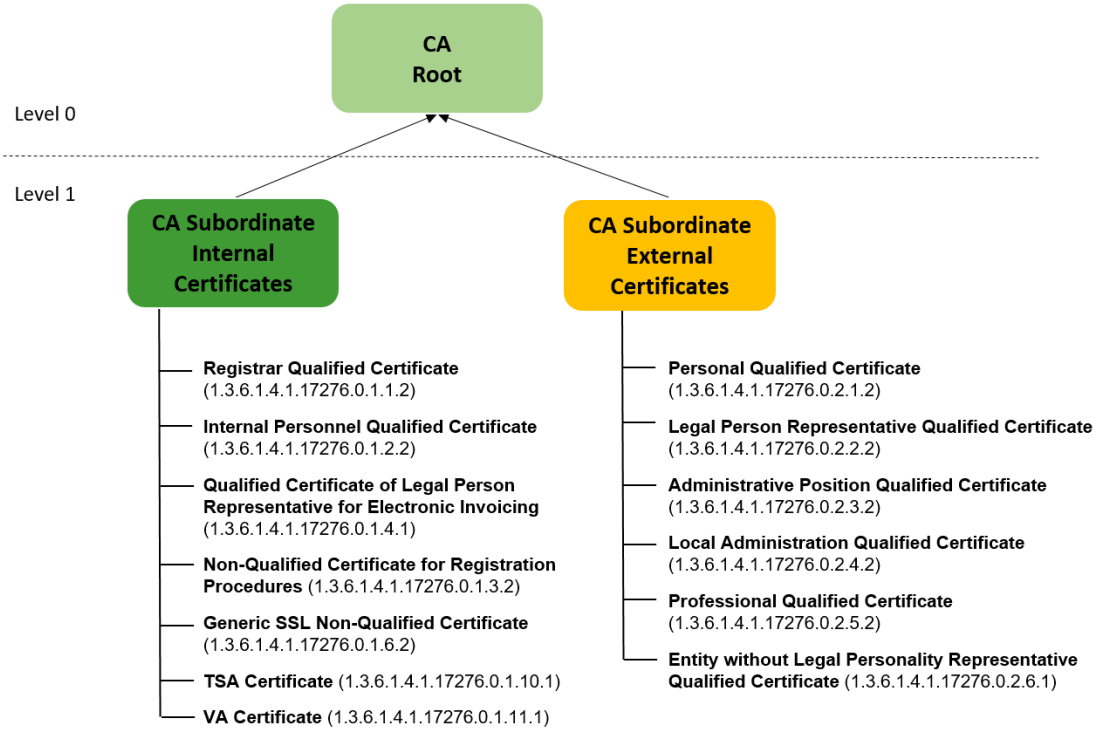
Colegio de Registradores de la Propiedad y Mercantiles de España

Prestador del Servicio de Certificación del Colegio de Registradores
C/ DIEGO DE LEON, 21.
28006-MADRID

The CORPME is, besides the provider (TSP), the CA (Certification Authority) in accordance with the applicable legislation, ley 59/2003, de 20 de diciembre de Firma Electrónica and The EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

Certification services are, in any case, applied in accordance with the principle of non-discrimination.

The general hierarchical architecture of the CORPME PKI is as follows:



1.3.2 Policy approval authority

The Policy Approval Authority (hereinafter PAA) is the organization responsible for the approval of the CPS and the CP's of CORPME, as well as the approval of the modifications of these documents.

In addition, the PAA is responsible, should it be necessary to evaluate the possibility of an external CA interacting with the CORPME PKI, to determine the adequacy of the CA's CPS to the affected Certification Policy.

The PAA is responsible for analyzing the reports of the audits, whether these are total or partial that are made of the PKI, as well as to determine, if necessary, the corrective actions to be performed.

The PAA will be formed by the Steering Committee, CORPME's highest governing body constituted by the following members:

- Member of the Coordination Service of the Clearing Offices of CORPME, acting as Chairman of the Committee.
- Vocal secretary of the CORPME.
- Member of the CORPME Business Registers Coordination Service.
- Member of the CORPME Information Systems Service.

1.3.3 Root Certification Authority

The CORPME issues all the certificates object of the CPS under the hierarchy of the Certificate of the main key, or root certificate. The root certificate is a self-signed certificate, with which the trust chain is started.

Subordinate to the Root, are the hierarchy or secondary key certificates, which will be one for the Internal Certificates and another for the External Certificates.

The holder of the Root Certificate is CORPME itself, and is issued and revoked by the Central Processing Unit, at the request of the Steering Committee, in accordance with the procedure defined in the PSC Rules of Procedure.

The most relevant information of the CORPME Root Certification Authority is the following:

Distinctive name	CN = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Serial Number	3b 38 d3 bf 57 b2 94 43 57 55 5d 78 9c fd 5e 5f
Issuer Name	CN = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Date of Issue	Monday 6th June 2016 13:24:40
Expiration Date	Wednesday 6th June 2040 13:24:40
RSA Key length	4096 Bits
Signature hash algorithm	SHA-512
Fingerprint (SHA-1)	97 4e 26 df 10 d2 c2 00 24 b2 1c 4a 0e b9 c7 ef 5c 06 80 d4
URL Publication certificate	http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt

1.3.4 Subordinate Certification Authorities

Under the hierarchy of the CORPME Root key or certificate, are the certificates of the Secondary Key for Internal Certificates and the Secondary Key for External Certificates, under whose respective hierarchies all certificates issued by CORPME are issued end entity.

The most relevant information of the subordinate CA for **Internal Certificates** is the following:

Distinctive name	CN = Autoridad de Certificación de los Registradores - AC Interna, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Serial Number	19 03 bc e3 42 82 77 60 57 55 8a f9 e9 b7 7e 2b
Issuer Name	CN = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Date of Issue	Monday 6th June 2016 16:38:48
Expiration Date	Wednesday 6th June 2028 16:38:48
RSA Key length	4096 Bits
Signature hash algorithm	SHA-512
Fingerprint (SHA-1)	11 bb d7 b4 a3 08 05 6e 15 13 20 1e 36 b6 9e a9 4e a9 f2 f9
URL Publication certificate	http://pki.registradores.org/certificados/ac_int_psc_corpme.crt
URL Publication CRL	http://pki.registradores.org/crls/crl_int_psc_corpme.crl
Types of certificates issued	**Registrar Qualified Certificate** (1.3.6.1.4.1.17276.0.1.1.2): the subscriber represents a natural person associated to a legal person.

	Internal Personnel Qualified Certificate (1.3.6.1.4.1.17276.0.1.2.2): the subscriber represents a natural person associated to a legal person. **Qualified Certificate of Legal Person Representative for Electronic Invoicing** (1.3.6.1.4.1.17276.0.1.4.1): the subscriber represents a natural person associated to a legal person, representing to this legal person. **Non-Qualified Certificate for Registration Procedures** (1.3.6.1.4.1.17276.0.1.3.2). **Generic SSL Non-Qualified Certificate** (1.3.6.1.4.1.17276.0.1.6.2). **TSA Certificate** (1.3.6.1.4.1.17276.0.1.10.1). **VA Certificate** (1.3.6.1.4.1.17276.0.1.11.1).

The most relevant information of the subordinate CA for **External Certificates** is the following:

Distinctive name	CN = Autoridad de Certificación de los Registradores - AC Externa, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Serial Number	0f 58 42 bf f2 91 93 45 57 55 91 64 34 56 36 54
Issuer Name	CN = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Broadcast Date	Monday 6th June 2016 17:06:11
Expiration Date	Wednesday 6th June 2028 17:06:11
RSA Key length	4096 Bits
Signature hash algorithm	SHA-512
Fingerprint (SHA-1)	e1 37 72 e5 a9 d6 2f 3f 5a 0a b1 ad ec 80 51 68 75 96 fb 70
URL Publication certificate	http://pki.registradores.org/certificados/ac_ext_psc_corpme.crt
URL Publication CRL	http://pki.registradores.org/crls/crl_ext_psc_corpme.crl
Types of certificates issued	**Personal Qualified Certificate** (1.3.6.1.4.1.17276.0.2.1.2): the subscriber represents a natural person. **Legal Person Representative Qualified Certificate** (1.3.6.1.4.1.17276.0.2.2.2): the subscriber represents a natural person associated to a legal person, representing to this legal person. **Administrative Position Qualified Certificate** (1.3.6.1.4.1.17276.0.2.3.2): the subscriber represents a natural person associated to a legal person. **Local Administration Qualified Certificate** (1.3.6.1.4.1.17276.0.2.4.2): the subscriber represents a natural person associated to a legal person. **Professional Qualified Certificate** (1.3.6.1.4.1.17276.0.2.5.2): the subscriber represents a natural person.

	Entity without Legal Personality Representative Qualified Certificate (1.3.6.1.4.1.17276.0.2.6.1): the subscriber represents a natural person associated to an organizational entity, which is not a legal person, representing to this entity.

1.3.5 Registration Authority

The Registration Authority of CORPME's PSC is formed by its Processing Units, and includes:

- Business Registry.
- Deaneries.
- Land Registry.
- Central Processing Unit.

They draw up the content of the certificates after making the necessary checks and authorize their issuance or revocation. For personal certificates, the Processing Units will generate in a secure device, the key cryptographic pairs for delivery to the Applicants.

All Processing Units will be under the supervision and direction of a registry owner, interim or accidental registrar, except;

- The Deaneries, whose head will be the Territorial Dean, or a registrar assigned by him.
- The Central Processing Unit, which will be responsible for any member of the Governing Board, appointed by the SSI member.

The Central Processing Unit will be in charge of the issuance or revocation of the device certificates (SSL), under request approved according to the procedure of request management and validated this request by the Technical Director of the SSI of CORPME.

All Registry Authorities operate under the supervision and coordination of the Steering Committee and require the prior authorization of the Board of Governors of CORPME, for the issuance of each class of certificates.

The issuance of certain digital certificates of CORPME will be verified, on request of online appointment of the Applicant, in the Internet address **https://pki.registradores.org/agenda**, in a single appearance, the day and time of your choice in the Processing Unit.

1.3.6 Validation authorities (VA)

The purpose of the Validation Authority (VA) is to facilitate the status of the certificates issued by the CORPME PSC through the Online Certificate Status Protocol (OCSP), which determines the current status of an electronic certificate at the request of an accepting third party without Require access to lists of certificates revoked by them.

This validation mechanism complements the publication of Revoked Certificate Lists (CRLs).

1.3.7 Time Stamping Authorities (TSA)

The Time Stamping Authority (TSA) is responsible for providing the services listed below, in a way that provides confidence to its users: Applicants, subscribers and third-party acceptors.

The services of time stamping are structured in two parts:

- **Provision of time stamps:** the technical and organizational components that issue the time stamps (TST).
- **Time stamps management:** the technical and organizational components that monitor and control the time stamp operation, including temporary synchronization with the UTC reference source.

The TSA is responsible for operating one or more Time Stamping Units (TSUs) which will create and sign the Time Stamps (TST) on behalf of the TSA. The TSA is identified in the electronic signature certificate that is used in the time stamp service.

1.3.8 End entities

Final entities are defined as natural person subjects to human rights, with sufficient capacity to request and obtain a CORPME digital certificate, in its own right or as a representative of a natural person or entity without legal personality. Also considered, as final entities are third parties in good faith who rely on CORPME certificates.

For the above purposes, they will be considered Final Entities:

- Applicant.
- Subscriber.
- Third Party who trusts in CORPME´s certificates.

1.3.8.1 Applicant

When a person is interested in obtaining a certificate issued by CORPME, they should complete the appointment request form of **https://pki.registradores.org/agenda** and acquire the status of a Requester. The mere request for a certificate does not imply the granting of the same, which is subject to the success of registration procedure before the corresponding Processing Unit, after verification of the information corresponding to the certificate that the Applicant provides.

Only senior citizens may request and, where appropriate; obtain digital certificates from CORPME.

1.3.8.2 Subscriber

Subscriber, in accordance with the provisions of article 6 of Law 59/2003 and regulation EU 910/2014, is the natural person whose identity is linked to a Data of creation and verification of Signature, through a Key Public certified (digitally signed) by the Trust Service Provider. Subscriber identification data is contained in the *Subject* field of the certificate defined within the ITU X509 standard.

Likewise, the person indicated in the following cases will have the consideration of Subscriber, for the purposes of the Law of Electronic Signature and of regulation EU 910/2014:

- In the case of the issuance of Certificates of Legal Entity Representative, the natural person who, by virtue of a power of attorney registered in the Mercantile Registry bears the representation of a juridical person, including the information of the latter in the certificate.
- In case of the issuance of Certificates of Entity without Legal Personality Representative, the natural person, by virtue of the appointment published in the Official State Gazette, including the data of this in the certificate.
- In the case of those specific profiles of certificates of Legal Entity Representatives issued to natural persons, the natural person who will accredit their capacity for their application and processing in the Central Processing Unit.

The Subscriber identity as the holder of the certificate will appear in the *Distinguished Name* field of the digital certificate in the CN (*Common Name*), SN (*Serial Number*), G (*Given Name*) and S (*Surname*) attributes, in the *Subject* field of the certificate. Subscriber identification data may also be included, depending on the type of certificate, in an extension of *subjectAltName,* in accordance with what is stipulated in the particular policies applicable to each certificate.

In the cases of representation of Legal Entities or Entities without Legal Personality, the data of the representation will be reflected in the *Description* attribute of the *Distinguished Name* field of the digital certificate.

1.3.8.3 Third parties that trust CORPME

For the purposes of this CP, Third Party is any user who relies on the certificates issued by the CORPME, and used for the signature of communications, electronic documents, or in the authentication to systems based on digital certificates.

The CORPME does not assume any liability to third parties, even in good faith, who have not applied the due diligence to verify the validity of the Certificates.

1.4 Certificate use

1.4.1 Appropriate use of certificates

The certificates regulated by this CP will be used to:

- **Authentication and Signature Certificates:** These certificates will be used for the authentication of people in front of the Information Systems of CORPME, the General Administration of the State and other type of Organisms and Entities, as well as for the generation of advanced electronic signatures.

1.4.2 Limitations and restriction on certificates use

Any use not included in the previous section is excluded.

1.5 Policies Administration

1.5.1 Responsible entity

The Information Systems Service (hereinafter SSI) through its Technical Advisory and Compliance Committee, constituted by;

- The Director of Technology and Systems, who acts as Chairman of the Committee.
- The Director of the Security and Regulatory Compliance Office, who will act as Secretary.
- The Director of Infrastructures, Security Engineering and Communications.
- The Director of Wintel Technology and Virtualization.
- The Director of Operations.
- A Director of Projects and Services, representing the Directors of Projects and Services.

The SSI must establish the terms and wording of the CORPME CPS. In those cases where applicable, in accordance with the TSP internal normative, the Steering Committee shall act by mandate of the CORPME Governance Board, or obtain its authorization in those matters whose competence is reserved to the Registrars governance.

The TSP Director will promote the convening of the Technical Advisory and Compliance Committee to transfer changes to the CPS and CP's of the CORPME's TSP or will be convened by the Committee itself.

The Technical Advisory and Compliance Committee shall carry out at least one annual review of these documents.

1.5.2 Procedure for approval and modification of the Certification Policies

The approval and subsequent modifications of the CP shall be the exclusive responsibility of the Steering Committee, in accordance with the powers delegated by the CORPME Governance Board, in accordance with the TSP internal normative.

Any modifications to this CP will be introduced and published on CORPME's website (**http://pki.registradores.org/normativa/index.htm**). Subscribers, who are dissatisfied with the modifications made, may request the revocation of their digital certificate.

The voluntary revocation by the user that is not in accordance with the provisions incorporated because of this CP will not grant the subscriber any right to be compensated for this reason.

1.6 Contact details

For queries or comments related to this CP, the interested party should contact CORPME through any of the following means:

Colegio de Registradores de la Propiedad y Mercantiles de España
Prestador de Servicios de Certificación del Colegio de Registradores
C/ DIEGO DE LEON, 21
28006-MADRID
E-mail: psc@registradores.org
Phone: +34 902181442 o +34 912701699

1.7 Definitions and Acronyms

1.7.1 Definitions

Advanced Electronic Signature: Electronic Signature establishing the personal identity of the Subscriber with respect to the signed data and verifying its integrity, as it is exclusively linked to both the Subscriber and the referred data, and be created by means that it can maintain under its exclusive control.

AEPD, Spanish Agency for Data Protection: Public Law entity, with its own legal personality and full public and private capacity whose purpose is to ensure compliance with legislation on the protection of personal data.

Applicant: Natural person who, after identification, requests the issuance of a Certificate.

Certificate Chain: Certificates list containing at least one Certificate and the CORPME Root Certificate.

Certificate Directory: Information repository following the ITU-T X.500 standard.

Certificate Revocation Lists or Revoked Certificate Lists (CRLs): List including exclusively the revoked or suspended (not expired) certificates relationships.

Certificate serial number: Integer and unique value unequivocally associated with a Certificate issued by CORPME.

Certificate: Electronic document electronically signed by a Trust Service Provider that links the Subscriber to a Signature Verification Data and confirms its identity. In this CP, where reference is made to a Certificate, it shall be understood as certificate issued by any CORPME Certification Authority.

Certification Authority: Natural or legal person that, in accordance with the legislation on Electronic Signature, issues Electronic Certificates, being able to also provide other services in relation to the Electronic Signature.

Certification Policy (CP): Document that completes the Certification Practice Statement, establishing the conditions of use and the procedures followed by CORPME to issue Certificates.

Certification Practice Statement (CPS): Declaration of CORPME available to the public electronically and free of charge as a Trust Service Provider in compliance with the provisions of the Law.

Cryptographic Card: A card used by the Subscriber to store private signature and decryption keys, to generate electronic signatures and decrypt data messages. It is considered a Secure Device for the creation of a Firm in accordance with the Law and allows the generation of a qualified Electronic Signature**.**

Electronic document: Set of logical records stored on a media susceptible to be read by electronic data processing equipment, containing information.

Electronic Signature: Set of data in electronic format, consigned together, that can be used as a mean of personal identification.

Hardware Security Cryptographic Module (HSM): Hardware module used to perform cryptographic functions and storing keys in safe mode.

Hash function: Operation performed on any size data set, so result obtained is another fixed size data set, regardless of the original size, and having the property of being uniquely associated with the initial data, i.e. it is impossible to find two different messages generating the same result when applying the Hash Function.

Hash or Fingerprint: Fixed-size result obtained after applying a hash function to a message fulfilling the property of being uniquely associated with the initial data.

ITU (International Telecommunication Union): International organization of the United Nations system in which governments and the private sector coordinate global telecommunication services and networks.

Key: Sequence of symbols.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: Law whose purpose is to guarantee and protect, with respect to the processing of personal data, public freedoms and fundamental rights of natural persons, and especially his honour and personal and family intimacy.

OCSP (Online Certificate Status Protocol): Computerized protocol that allows checking the status of a Certificate at the time it is used.

OCSP Request: Request for a Certificate status to OCSP Responder by Following the OCSP Protocol.

OCSP Responder: Computer server that responds, following the OCSP protocol, to the OCSP Requests with the status of the Certificate consulted.

OID (Object IDentifier): Value, hierarchical and with a comprehensive a sequence of variable components, consisting of nonnegative integers separated by a point that can be assigned to registered objects and having the property of being unique among the rest of OID.

PIN (Personal Identification Number): Specific number known only by the person who has to access a resource and protected by this mechanism.

PKCS # 10 (Certification Request Syntax Standard): Standard developed by RSA Labs, and internationally accepted, which defines the syntax of a Certificate request.

Policy: For the purposes of the Certification Practice Statement, the Policy is the notarial document that documents the notarial intervention as Registration Authority before the subscriber, as well as his intervention in the case of revocation of the same.

Public Key Infrastructure (PKI): Infrastructure that supports the management of Public Keys for authentication, encryption, integrity, or non-repudiation services.

PUK: (Personal Unblocking Key) Specific number or key only known by the person who has to access a resource that is used to unblock access to that resource.

Qualified Certificate: Certificate issued by a Trust Service Provider complying with the requirements established in the Law in terms of the verification of the identity and other circumstances of the Applicants and the reliability and guarantees of the certification services they provide.

Qualified Electronic Signature: Advanced Electronic Signature based on a qualified Certificate generated by a Secure Signature Creation Device.

Qualified Signature Creation Device: Instrument used to apply the Signature Creation Data, complying with the requirements set out in Annex III of Directive 1999/93 / EC of the European Parliament and of the Council of 13 December 1999, and with the specific rules applicable in Spain.

Registration Authority: Entity who, having an agreement with the CORPME, is in charge of verifying the identity of the Certificates Applicants and Subscribers, and if applicable, also the validity of powers of representatives and subsistence of legal persons or voluntary representatives.

Responsible for Security: Person in charge of coordinating and controlling the measures defined by the Security Document regarding the files.

Responsible for the File (or File Treatment): Person who decides the purpose, content and use of the file treatment.

Responsible for Treatment: Natural or Legal person, public authority, service or any other body treating personal data on behalf of the Person in charge of the processing of the Files.

Root Certificate: Certificate whose Subscriber is a Certification Authority belonging to the CORPME hierarchy as Trust Service Provider, and containing the Signature Verification Data of that Authority signed with the Signing Data as the Trust Service Provider.

Security document: Document required by the LOPD, whose purpose is to establish the security measures implemented, for the purposes of this document, by CORPME as Trust Service Provider, for the protection of personal data contained in the Activity files containing personal data (hereinafter the Files).

SHA-1: Secure Hash Algorithm (secure algorithm of summary -hash-). Developed by NIST and revised in 1994 (SHA-1). The algorithm consists of taking messages of less than 264 bits and generating a summary of 160 bits in length. The probability of finding two different messages producing a single summary is practically null. For this reason, it is used to ensure the integrity of the documents during the process of Electronic Signature.

Signature creation data (Private Key): Unique data, such as codes or private cryptographic keys, used by the signer to create the Electronic Signature.

Signature verification data (Public Key): Data, such as public cryptographic codes or keys, which are used to verify the Electronic Signature.

Subscriber (or Subject): The holder or signer of the Certificate. The person whose personal identity is linked to the electronically signed data, through a Public Key certified by the Trust Service Provider. The concept of Subscriber will be referred in the Certificates and in the computer applications related to the issuance as Subject, for strict reasons of international standardization.

Third parties relying on Certificates: Those who place their trust in a CORPME Certificate, verifying the validity of the Certificate as described in the CPS.

Time Stamping: Confirmation of date and time in an electronic document using cryptographic means based on “Request for comments**:** 3161 - "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", which manages to date the date and time in an objective manner.

Trust Service Provider: Natural or Legal person who, in accordance with the legislation on Electronic Signature, issues Electronic Certificates, is able to also provide other services in relation to the Electronic Signature. In this CP, it will correspond with the Certification Authorities belonging to the CORPME hierarchy.

X.500: Standard developed by the ITU that defines the directory recommendations. It corresponds to the ISO / IEC 9594-1: 1993 standard. It gives rise to the following set of recommendations: X.501, X.509, X.511, X.518, X.519, X.520, X.521 and X.525.

X.509: Standard developed by the ITU, which defines the basic electronic format for Electronic Certificates.

1.7.2 Acronyms

C: Country. Distinctive Name (DN) attribute of an object within the X.500 directory structure.

CA: Certification Authority.

CDP: CRL Distribution Point.

CN: Common Name. Distinctive Name (DN) attribute of an object within the X.500 directory structure.

CORPME: The Public Corporation of Land and Business Registers of Spain.

CP: Certificate Policy.

CPS: Certification Practice Statement.

CRL: Certificate Revocation List.

CSR: Certificate Signing Request. A set of data, containing a public key and its Electronic Signature using the associated private key, sent to the Certification Authority for the issuance of an electronic certificate containing such public key.

CWA: CEN Workshop Agreement.

DN: Distinguished Name. Uniquely identifies an entry in an X.500 directory.

FIPS: Federal Information Processing Standard.

HSM: Hardware Security Module. Cryptographic security module used for key storage and safe cryptographic operations.

IANA: Internet Assigned Numbers Authority.

IETF: Internet Engineering Task Force (Internet Standardization Organization).

ITU: International Telecommunication Union.

O: Organization. Distinctive Name (DN) attribute of an object within the X.500 directory structure.

OCSP: Online Certificate Status Protocol. Protocol for online verification of the validity of an electronic certificate.

OID: Object Identifier.

OU: Organizational Unit. Distinctive Name (DN) attribute of an object within the X.500 directory structure.

PAA: Policy Approval Authority.

PIN: Personal Identification Number. Password that protects access to a cryptographic device.

PKCS: Public Key Cryptography Standards. PKI standards developed by internationally accepted RSA laboratories.

PKI: Public Key Infrastructure.

PUK: PIN Unlock Key. Password that allows unlocking a cryptographic device blocked by having repeatedly entered a wrong PIN consecutively.

RA: Registration Authority.

RFC: Request for Comments. Standard developed by the IETF.

ROA: Real Observatorio de la Armada Española (Royal Observatory of the Spanish Navy).

SSI: Information Systems Service of the CORPME.

SSL: Secure Sockets Layer.

TSA: Time Stamping Authority.

TSP: Trust Service Provider.

TST: Time Stamp Token.

TSU: Time Stamping Unit.

UTC: Universal Time Coordinated.

VA: Validation Authority.

2 DIRECTORY AND PUBLICATION OF CERTIFICATES

2.1 Certificate validation directory

The CORPME maintains a Certificate Validation Directory permanently available and accessible to all interested parties, in accordance with current regulations. In order to guarantee a continuous and uninterrupted access to the certificate verification service, the Directory server is duplicated and balanced, therefore , in the event of a service failure or fall, the second directory will be immediately posted online, thus guaranteeing itself The availability of the same.

The Certificate Validation Directory is a public directory of inquiry, containing all the CRLs issued by the Trust Service Provider, whose validity period is not expired, including the date and time when revocation took place.

No more limitations on access to the Directory will be established than those imposed for security reasons.

ARL	**http://pki.registradores.org/crls/arl_psc_corpme.crl**
CRL CA Internal Certificates	**http://pki.registradores.org/crls/crl_int_psc_corpme.crl**
CRL CA External certificate	**http://pki.registradores.org/crls/crl_ext_psc_corpme.crl**
Online validation service implementing the OCSP protocol	**http://ocsp.registradores.org and https://ocsp.registradores.org**
Time Stamping Protocol Service	**http://tsa.registradores.org and https://tsa.registradores.org**
Certificate CORPME certification Authority	**http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt**
Internal CA certificate	**http://pki.registradores.org/certificados/ac_int_psc_corpme.crt**
External CA certificate	**http://pki.registradores.org/certificados/ac_ext_psc_corpme.crt**
Certification Practice and Policies	**http://pki.registradores.org/normativa/index.htm**

2.2 Publication of certification information

The Directory is published in accordance with the Lightweight Directory Access Protocol (LDAP) standard, and it will include the published ARL, and the published CRLs, following the X.509 standard (Certificate Revocation List, version 2). The Online Certificate Status Protocol (OCSP) can also be used.

The revoked certificate lists will be updated periodically as indicated in section 4.9.7 of this document.

2.3 Publication Frequency

The CPS and the Certification Policies will be published at the time of their creation and will be republished at the time of approval of any changes on them. The modifications will be made public in the Web Directory referenced in section 2.1 of this document.

The CA will add revoked certificates to the relevant CRL within the time stipulated in section 4.9.7 of this document.

2.4 Access Controls for Certification Information

The access for the consultation of the CPS and CP's is public for all interested parties. The CORPME will have the necessary security measures to prevent unauthorized manipulation of these documents. Those documents will also be digitally signed by a certificate issued by the CORPME to guarantee its integrity.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Names

3.1.1 Names Types

All certificate holders require a distinctive name (*Distinguished Name*) conforming to the X.500 standard.

3.1.1.1 Registrar Qualified Certification

The structure of the certificate, referring to the certificate *Subject* field, is the one described in the following table:

Field	Value	Description
C	ES	Country.
organizationIdentifier	VATES-Q2863012G	NIF (Required by ETSI 319 412-2).
O	Colegio de Registradores de la Propiedad y Mercantiles	Organization.
OU	*NAME OF THE REGISTRY*	Registry in which the certificate holder performs his function. All data must be in UPPERCASE.
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Required by ETSI EN 319 412-2.
SN	*SURNAME*	**surname.** Required by ETSI EN 319 412-2. All data must be in UPPERCASE.
G	*NAME*	**givenName.** Required by ETSI EN 319 412-2. All data must be in UPPERCASE.
CN	NOMBRE *NAME SURNAME*– NIF *NIF*	All data must be in UPPERCASE.

3.1.1.2 Internal Personnel Qualified Certificate

The structure of the certificate, referring to the certificate *Subject* field, is the one described in the following table:

Field	Value	Description
C	ES	Country.
organizationIdentifier	VATES-Q2863012G	NIF (Required by ETSI 319 412-2).
O	Colegio de Registradores de la Propiedad y Mercantiles	Organization.
OU	*NAME OF THE REGISTRY OR DESTINATION UNIT*	All data must be in UPPERCASE.
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Required by ETSI EN 319 412-2.
SN	*SURNAME*	**surname.** Required by ETSI EN 319 412-2. All data must be in UPPERCASE.
G	*NAME*	**givenName.** Required by ETSI EN 319 412-2. All data must be in UPPERCASE.
CN	NOMBRE *NAME SURNAME* – NIF *NIF*	All data must be in UPPERCASE.

3.1.1.3 Qualified Certificate of Legal Person Representative for Electronic Invoicing

The structure of the certificate, referring to the certificate *Subject* field, is the one described in the following table:

Campo	Valor	Descripción
C	ES	Country.
description	Reg: Registro salida CORPME /Fecha: *DD-MM-AAAA* /Numero: *NUM*	Official document Codification that accredits the powers of the signer and its registration in the file of the CORPME.
organizationIdentifier	VATES-*NIF*	Entity NIF (@signature and Required by ETSI 319 412-2).
O	*BUSINESS NAME*	Organization for @firma (Required by ETSI 319 412-2). All data must be in UPPERCASE.

SERIALNUMBER	IDCES-*DNI / NIE / PASSPORT*	**serialNumber.** Required by ETSI EN 319 412-2.
SN	*SURNAME*	**surname.** Required by ETSI EN 319 412-2. All data must be in UPPERCASE.
G	*NAME*	**givenName.** Required by ETSI EN 319 412-2. All data must be in UPPERCASE.
CN	*DNI NAME SURNAME* (R: *NIF*)	All data must be in UPPERCASE. The field has a maximum length of 64 characters in accordance with RFC 5280.

3.1.1.4 Non-Qualified Certificate for Registration Procedures

The structure of the certificate, referring to the certificate *Subject* field, is the one described in the following table:

Field	Value	Description
C	ES	Country
organizationIdentifier	VATES-Q2863012G	NIF (Required by ETSI 319 412-2)
O	Colegio de Registradores de la Propiedad y Mercantiles	Organization
CN	*NAME OF THE REGISTRY*	Registry holding the certificate. All data must be in UPPERCASE.

3.1.1.5 Generic SSL Non-Qualified Certificate

The structure of the certificate, referring to the certificate *Subject* field, is the one described in the following table:

Field	Value	Description
C	ES	Country
organizationIdentifier	VATES-Q2863012G	NIF (Required by ETSI 319 412-2)

O	Colegio de Registradores de la Propiedad y Mercantiles	Organization
CN	*<Nombre Máquina / Nombre DNS>*	

3.1.2 Need for names to be meaningful

In all cases, the distinctive certificate holder's names must be significant, in accordance with the rules imposed in previous section.

3.1.3 Rules for Interpreting name formats

The rule used by the CORPME TSP to interpret the distinguished names of the certificate holders is ISO / IEC 9595 (X.500) *Distinguished Name* (DN).

3.1.4 Uniqueness of names

The *Distinguished Name* set and the contents of *Policy Identifier* extension must be unique and unambiguous.

- For Registrar Qualified Certificates, the name use (composed of surnames and the name), and of NIF in CN guarantees the uniqueness of the same.
- For Internal Personnel Qualified Certificates, the name use (composed of surnames and name), and NIF, NIE, passport or other identification document in CN guarantees the uniqueness of the same.
- Non-Qualified Certificate for Registration Procedures, the name use of the registry holder of the certificate in CN, guarantees the uniqueness of the same.
- For Generic SSL Non-Qualified Certificate, the use of the machine name in CN, guarantees the uniqueness of the same.
- Qualified Certificates of Legal Person Representative for Electronic Invoicing, the entity use (composed of the company name), the NIF, the name (composed of surnames and name), and the NIF (composed of NIF, NIE, passport or other) in CN guarantees the uniqueness of the same.

3.1.5 Conflict resolution procedure

Any dispute concerning names ownership shall be solved as set forth in paragraph 9.13 of this document.

3.1.6 Recognition, authentication and trademarks role

Not stipulated.

3.2 Initial identity validation

3.2.1 Private Key Possession Proof

The private keys of the following internal certificates,

- Registrar Qualified Certificate.

- Internal Personnel Qualified Certificate.
- Qualified Certificate of Legal Person Representative for Electronic Invoicing.

will be generated by Applicant's secure cryptographic device in his custody. Within these devices, both the key generation and the signature cryptographic operations will be carried out, directly and immediately. Thus, in no case will be necessary to transfer the private key to an external device, guaranteeing the subscriber his / her absolute control over the signature creation data, and, therefore, the impossibility of impersonation of his / her electronic signature. The order for generating the keys and the introduction of the passwords in the cryptographic device will be carried out personally by the certificate holder.

For Generic SSL Non-Qualified Certificates, the CORPME will verify that the requester has the private key corresponding to the public key related to the requested Certificate.

For Non-Qualified Certificates for Registration Procedures, the CORPME will verify by means of the receipt of the license of use signed by the corresponding Registry holder, that the Applicant has the private key corresponding to the public key related to the requested Certificate.

3.2.2 Authentication of Identity for Legal Persons

The national applicants for CORPME's Certificates must appear before the Processing Unit of their choice, with their NIF, NIE, passport or other identification document.

Foreign applicants for CORPMES's Certificates, must present, with their foreign identification number (NIE), or their passport, or their residence card or any other legal document of identification.

Besides the applicant identification by checking the above mentioned documentation, the corresponding Processing Unit Responsible must request the documentation proving the certifiable attribute depending on the type of certificate.

3.2.3 Authentication of Identity for Natural Persons

The Applicant must provide the following information, depending on certificate requested:

3.2.3.1 Registrar Qualified Certificate

- Name of the Registry(registry in which the certificate holder exercises his or her function).
- Subscriber's name and surname.
- Identity document (DNI / NIF / National Passport) of the subscriber.
- Email.
- Phone number.
- Postal address (optional).
- Windows Primary Name (UPN) (optional).
- Position.
    - Active Registrar
        - Certificate issued online confirming the corresponding position.

3.2.3.2 Internal Personnel

- Name of the Registry or Destination Unit

- In the case of Registrar employees: Registrar in which the holder of the certificate exercises its function.
- In the case of Deanery employees: Deanery in which the holder of the certificate exercises its function.
- In the case of CORPME employees, positions of the CORPME, positions of the CORPME Governance board, aspirant Registrars, retired Registrars, Registrar on voluntary leave and employees of CORPME related associations, personnel of external organizations providing services to CORPME: CORPME.

- Subscriber's name and surname.
- Identification document of the subscriber.
  - In case of positions of CORPME Governance Board, aspirant registrars, retired Registrars, Registrar on voluntary leave: DNI / NIF / National Passport.
  - In the case of CORPME employees, registrar employees, deanery employees, positions of the CORPME and employees of associations related to the CORPME, personnel of external organizations providing services to CORPME: DNI / NIF / Passport / NIE.
- Email.
- Phone number.
- Postal address (optional).
- Windows Primary Name (UPN) (optional).
- Subtype: College, Register, Organization (associations related to the CORPME), aspirant registrars, retired registrars, Registrar on voluntary leave, personnel of external organizations providing services to CORPME.
- Business Name (if applicable).
- Position.
  - CORPME employee.
    - Declaration of Responsibility issued by the Vice-Dean or CORPME´s Human Resources Director confirming the position.
  - Employee of Land or Business Registry.
    - Declaration of Responsibility issued by the Registrar confirming the position.
  - Position of the CORPME.
    - Declaration of Responsibility issued by the Vice-Dean or CORPME´s Human Resources Director confirming the position Position.
  - Position of the CORPME Governance board.
    - Declaration of Responsibility issued by the CORPME Secretary confirming the position.
  - Aspirant registrar.
    - Certificate issued online confirming the position.
  - Retired Registrar.
    - Certificate issued online confirming the position.
  - Registrar on Voluntary leave.
    - Certificate issued online confirming the position.
  - Personnel of external organizations providing services to CORPME.

- Certificate from the external organization specifying the personnel identity and their assignment to services provided to CORPME TSP. This certificate will be provided by CORPME SSI Chief Financial Officer, as responsible of third parties agreements.

3.2.3.3 Qualified Certificate of Legal Person Representative for Electronic Invoicing

- Subscriber's name and surname.
- Subscriber's Identity document (DNI / NIF / National Passport).
- Email.
- Phone number.
- Postal address (optional).
- Business name.
- CORPME NIF.
- Position.
  - CORPME Dean-President.
    - Declaration of Responsibility issued by the CORPME Secretary confirming the position and,
    - Copy of CORPME Log out record with official notification to the Head of the Registrars and Notary of the Dean-President nomination.
- Issue number.
- Issue date of the document.

3.2.4 Authentication of Device Identity

3.2.4.1 Non-Qualified Certificate for Registration procedures

- Name of Registry holding the certificate.
- Email (optional).
- Postal address.
- Operator.

3.2.4.2 Generic SSL Non-Qualified Certificate

- Machine Names or DNS Names.
- Email.

3.2.5 Information not verified about the Applicant

All information presented by an Applicant is verified before the certificate issuance.

3.2.6 Representation powers verification

Besides the Applicant identification by checking the above mentioned documentation, the corresponding Processing Unit Responsible must request the documentation proving the certifiable attribute depending on the type of certificate.

The Processing Unit will verify the equivalence of the certification in the terms of the certificate, as well as the exact correlation between the validity periods of the registered attribute and the certificate. If an inaccuracy is detected, it will revoke the certificate within this period, notifying the holder of this fact.

3.2.7 Criteria for operating with external CAs

As specified in the CORPME Certification Practice Statement (CPS).

3.3 Identification and authentication for renewal requests

The Holders identification and authentication for the renewal requests are specified in section 4.7 of this document.

3.4 Identification and authentication for revocation request

The holders identification and authentication the revocation requests are specified in section 4.9 of this document.

4 OPERATIONAL REQUIREMENTS FOR CERTIFICATES LIFE CYCLE

4.1 Application for certificates

4.1.1 Who can make an application

The request will vary according to the type of Qualified Certificate requested.

In addition, to the information indicated in the following sections, the subscriber authorized legal representative, duly authorized, may also make a certificate request.

For request of some of the certificates issued by CORPME, a prior appointment may be required.

4.1.1.1 Registrar Qualified Certificate

The request for this type of certificate may be made by active Registrars.

The request process does not require a prior appointment. The request will be made by the creation of a fake appointment to request and validate the user's data and proceed to invoke the issuance of the certificate.

Users requesting qualified certificates will be issued with a corresponding identification document and a certificate accrediting the position, and for applications for unqualified certificates, the request will be sent by e-mail, and will be issued by the Central Processing Unit of the CORPME.

4.1.1.2 Internal Personnel Qualified Certificate

The request for this type of certificate may be made by CORPME employees, Registry employees, Deanery employees, and positions of the CORPME, positions of the CORPME Governance Board, aspirant Registrars, retired Registrars, Registrars on voluntary leave and employees of CORPME related associations, personnel of external organizations providing services to CORPME.

The request process does not require a prior appointment. The request will be made by the creation of a fake appointment to request and validate the user's data and proceed to invoke the issuance of the certificate.

Users requesting qualified certificates will be issued with a corresponding identification document and a certificate accrediting the position, and for applications for unqualified certificates, the request will be sent by e-mail, and will be issued by the Central Processing Unit of the CORPME.

4.1.1.3 Qualified Certificate of Legal Person Representative for Electronic Invoicing

The request for this type of certificate may be made by the Dean-President of the Registrar's Association.

The request process does not require a prior appointment. The request will be made by the creation of a fake appointment to request and validate the user's data and proceed to invoke the issuance of the certificate.

Users requesting qualified certificates will be issued with a corresponding identification document and a certificate accrediting the position, and for applications for unqualified certificates, the request will be sent by e-mail, and will be issued by the Central Processing Unit of the CORPME.

4.1.1.4 Non-Qualified Certificate for Registration Procedures

Certificates Not Qualified for Registration Procedures will be issued from Central Processing Unit. Certificate issuance batches will be generated and once generated, a script will be executed to change the PKCS # 12 password with a unique random password for each one.

From CORPME core services, the certificates will be installed on the integration servers of each registry and once the operation is completed, the PKCS # 12 password will be notified to the registry security manager so that they can be installed in the registry servers. Registry clients.

After the period of one week will proceed to the revocation of the certificates that have been renewed.

The Central Processing Unit, once the certificates have been installed, will erase any references to these and their respective passwords, to ensure non-repudiation.

4.1.1.5 Generic SSL Non-Qualified Certificate

For Generic SSL Non-Qualified Certificates issuance, a request must be sent through the corporate email to the CORPME Central Processing Unit.

The Central Processing Unit will proceed to process the request, validating this request the Technical Director of the SSI and checking if there is another certificate of the same class and with same holder name. If so, proceed to deny the request. Finally, the Central Processing Unit will notify the Applicant the approval or the denial of the request.

In case the request is positive, the issued certificate will be provided, and a license will be sent twice in electronic format, both signed by the Applicant and returned by one of the copies. A application and license copy shall remain in the holder possession and the other shall be filed in the Central Processing Unit, for a period of fifteen (15) years.

4.1.2 Registration of requests and applicant´s responsibilities

As specified in CORPME Certification Practice Statement (CPS).

4.2 License Applications Processing

4.2.1 Performing identification and authentication function

As specified in CORPME Certification Practice Statement (CPS).

4.2.2 License application approval or rejection

As specified in CORPME Certification Practice Statement (CPS).

4.2.3 Deadline for license applications processing

As specified in CORPME Certification Practice Statement (CPS).

4.3 Certificates Issuance

4.3.1 CA actions during certificate issuance

As specified in CORPME Certification Practice Statement (CPS).

4.3.2 Issuance notification to the Applicant by CA of certificate

As specified in CORPME Certification Practice Statement (CPS).

4.4 Certificate acceptance

4.4.1 Certificate acceptance mechanism

As specified in CORPME Certification Practice Statement (CPS).

4.4.2 Publication of certificate

As specified in CORPME Certification Practice Statement (CPS).

4.4.3 Certificate issuance notification by CA to other authorities

As specified in CORPME Certification Practice Statement (CPS).

4.5 Private Key and certificate use

As specified in CORPME Certification Practice Statement (CPS).

4.5.1 Use of the private key and certificate by the holder

As specified in CORPME Certification Practice Statement (CPS).

4.5.2 Public key and certificate Use by third party acceptors

As specified in CORPME Certification Practice Statement (CPS).

4.6 Certificate Renewals without Key Change

4.6.1 Circumstances for renewal of certificates without Key change

Not stipulated.

4.6.2 Who can request renewal of certificate without key change

Not stipulated.

4.6.3 Certificate Renewal Request without key Change Processing

Not stipulated.

4.6.4 Notification of issue of a renewal certificate to holder

Not stipulated.

4.6.5 Acceptance form of certificate without keys change

Not stipulated.

4.6.6 Publication of the certificate without CA change

Not stipulated.

4.6.7 Certificate renewal notification by CA to other authorities

Not stipulated.

4.7 Renewing certificates with key changes

As specified in CORPME Certification Practice Statement (CPS).

4.7.1 Circumstance for renewal with certificate changing keys

As specified in CORPME Certification Practice Statement (CPS).

4.7.2 Who can request renewal of certificates with change of keys

As specified in CORPME Certification Practice Statement (CPS).

4.7.3 Processing of certificate renewal requests with keys change

As specified in CORPME Certification Practice Statement (CPS).

4.7.4 Notification of renewal of a new certificate to holder

As specified in CORPME Certification Practice Statement (CPS).

4.7.5 Acceptance of certificate with change of key

As specified in CORPME Certification Practice Statement (CPS).

4.7.6 Publication of the certificate with key change by the CA

As specified in CORPME Certification Practice Statement (CPS).

4.7.7 Notification of the renewal of the certificate by CA to other Authorities

As specified in CORPME Certification Practice Statement (CPS).

4.8 Certificates modification

As specified in CORPME Certification Practice Statement (CPS).

4.8.1 Circumstances for certificate modification

Not stipulated.

4.8.2 Who can request certificate modification

Not stipulated.

4.8.3 Processing of certification modification request

Not stipulated.

4.8.4 Notification of the modification of a certificate to the holder

Not stipulated.

4.8.5 Acceptance of the modified certificate

Not stipulated.

4.8.6 Publication of certificate modified by CA

Not stipulated.

4.8.7 Notification of the modification of the certificate by the CA to other Authorities

Not stipulated.

4.9 Revocation and suspension of certificates

4.9.1 Circumstances for revocation

As specified in CORPME Certification Practice Statement (CPS).

4.9.2 Who can request revocation

As specified in CORPME Certification Practice Statement (CPS).

4.9.3 Revocation request procedure

As specified in CORPME Certification Practice Statement (CPS).

4.9.4 Grace Period of the Revocation Request

As specified in CORPME Certification Practice Statement (CPS).

4.9.5 Term on which the CA must resolve the revocation request

As specified in CORPME Certification Practice Statement (CPS).

4.9.6 Verification requirement for revocation by trusted third parties

As specified in CORPME Certification Practice Statement (CPS).

4.9.7 CRL emission Frequency

As specified in CORPME Certification Practice Statement (CPS).

4.9.8 Maximum time between CRL generation and publication

As specified in CORPME Certification Practice Statement (CPS).

4.9.9 Availability of online system for verifying certificate status

In addition to the publication of the CRLs, CORPME has an OCSP certificate validation service, which implements the "*RFC6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol*", in which the revocation status of a certain certificate issued by the TSP of CORPME. The access URL is published in the CORPME Certification Practice Statement (CPS).

4.9.10 Online Revocation Checking Requirements

As specified in CORPME Certification Practice Statement (CPS).

4.9.11 Other forms of disclosure of revocation information available

As specified in CORPME Certification Practice Statement (CPS).

4.9.12 Special Requirement for Committed Key revocation

As specified in CORPME Certification Practice Statement (CPS).

4.9.13 Causes for suspension

As specified in CORPME Certification Practice Statement (CPS).

4.9.14 Who can request suspension

As specified in CORPME Certification Practice Statement (CPS).

4.9.15 Procedure for requesting suspension

As specified in CORPME Certification Practice Statement (CPS).

4.9.16 Limits of the suspension period

As specified in CORPME Certification Practice Statement (CPS).

4.10 Certificate status Information Services

4.10.1 Operating characteristics

As specified in CORPME Certification Practice Statement (CPS).

4.10.2 Service Availability

As specified in CORPME Certification Practice Statement (CPS).

4.10.3 Additional Features

As specified in CORPME Certification Practice Statement (CPS).

4.11 Expiry of the validity of a certificate

As specified in CORPME Certification Practice Statement (CPS).

4.12 Custody and keys recovery

4.12.1 Custody and recovery policies and practices

Not stipulated.

4.12.2 Session Key protection and recovery Policies and Practices

Not stipulated.

5 PHYSICAL SECURITY CONTROLS, INSTALLATIONS, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical controls

As specified in CORPME Certification Practice Statement (CPS).

5.1.1 CORPME Facilities location and physical security measures

As specified in CORPME Certification Practice Statement (CPS).

5.1.2 Physical access

As specified in CORPME Certification Practice Statement (CPS).

5.1.3 CORPME Facilities electrical supply and environmental conditioning

As specified in CORPME Certification Practice Statement (CPS).

5.1.4 Exposure to water

As specified in CORPME Certification Practice Statement (CPS).

5.1.5 Measures against fires and floods

As specified in CORPME Certification Practice Statement (CPS).

5.1.6 Storage system

As specified in CORPME Certification Practice Statement (CPS).

5.1.7 Waste Disposal

As specified in CORPME Certification Practice Statement (CPS).

5.1.8 Information Backup Policy

As specified in CORPME Certification Practice Statement (CPS).

5.2 Procedural controls

As specified in CORPME Certification Practice Statement (CPS).

5.2.1 Responsible roles for CORPME PKI control and management

As specified in CORPME Certification Practice Statement (CPS).

5.2.2 Number of persons required per task

As specified in CORPME Certification Practice Statement (CPS).

5.2.3 Roles requiring segregation of functions

As specified in CORPME Certification Practice Statement (CPS).

5.3 Personnel controls

As specified in CORPME Certification Practice Statement (CPS).

5.3.1 Requirement for professional qualifications, knowledge and experience

As specified in CORPME Certification Practice Statement (CPS).

5.3.2 Background Check Procedures

As specified in CORPME Certification Practice Statement (CPS).

5.3.3 Training requirements

As specified in CORPME Certification Practice Statement (CPS).

5.3.4 Requirements and frequency of training update

As specified in CORPME Certification Practice Statement (CPS).

5.3.5 Frequency and Rotation Sequence of Tasks

As specified in CORPME Certification Practice Statement (CPS).

5.3.6 Penalties for unauthorized actions

As specified in CORPME Certification Practice Statement (CPS).

5.3.7 Requirements for contracting third parties

As specified in CORPME Certification Practice Statement (CPS).

5.3.8 Documentation provided to staff

As specified in CORPME Certification Practice Statement (CPS).

5.4 Security Audit Procedures

As specified in CORPME Certification Practice Statement (CPS).

5.4.1 Registered event types

As specified in CORPME Certification Practice Statement (CPS).

5.4.2 Frequency of processing audit record

As specified in CORPME Certification Practice Statement (CPS).

5.4.3 Audit records retention period

As specified in CORPME Certification Practice Statement (CPS).

5.4.4 Audit records protection

As specified in CORPME Certification Practice Statement (CPS).

5.4.5 Procedures for supporting audit record

As specified in CORPME Certification Practice Statement (CPS).

5.4.6 Notification to subject causing the event

As specified in CORPME Certification Practice Statement (CPS).

5.4.7 Vulnerability Analysis

As specified in CORPME Certification Practice Statement (CPS).

5.5 Archiving records

As specified in CORPME Certification Practice Statement (CPS).

5.5.1 Archived events types

As specified in CORPME Certification Practice Statement (CPS).

5.5.2 Record retention period

As specified in CORPME Certification Practice Statement (CPS).

5.5.3 File protection

As specified in CORPME Certification Practice Statement (CPS).

5.5.4 File Backup Procedures

As specified in CORPME Certification Practice Statement (CPS).

5.5.5 Requirements for time stamping of records

As specified in CORPME Certification Practice Statement (CPS).

5.5.6 File information system (internal vs. External)

As specified in CORPME Certification Practice Statement (CPS).

5.5.7 Procedures for obtaining and verifying archived information

As specified in CORPME Certification Practice Statement (CPS).

5.6 Change of keys

As specified in CORPME Certification Practice Statement (CPS).

5.7 Recovery from key or catastrophic commitment

As specified in CORPME Certification Practice Statement (CPS).

5.7.1 Incident and commitment management procedures

As specified in CORPME Certification Practice Statement (CPS).

5.7.2 Alteration of hardware, software and / or data resources

As specified in CORPME Certification Practice Statement (CPS).

5.7.3 Procedure of action against the commitment of the Authority private key

As specified in CORPME Certification Practice Statement (CPS).

5.7.4 Installation after a natural disaster or other catastrophe

As specified in CORPME Certification Practice Statement (CPS).

5.8 CA or RA Termination

As specified in CORPME Certification Practice Statement (CPS).

5.8.1 CA Termination

As specified in CORPME Certification Practice Statement (CPS).

5.8.2 RA Termination

As specified in CORPME Certification Practice Statement (CPS).

6 TECHNICAL SECURITY CONTROLS

6.1 Generating and installing the key pair

6.1.1 Generation of the key pair

Subscriber keys, which will have a length of 2048 bits for all certificates.

Qualified Certificates (Registrars, Internal Personnel and Legal Person Representative for Electronic Invoicing) are always generated during the appearance of the Applicant and with their personal intervention in the process of assigning keys.

For Non-Qualified Certificates (Registration Procedures and SSL) the personal appearance of the Applicant is not necessary and the keys will be generated in the device and a request for a certificate that will be provided to the Central Processing Unit.

6.1.2 Delivery of private key to holder

As specified in CORPME Certification Practice Statement (CPS).

6.1.3 Delivery of public key to certificate issuer

As specified in CORPME Certification Practice Statement (CPS).

6.1.4 Delivery of CA public key to trusted third parties

The CORPME TSP CAs public key is available to third parties who rely on the CORPME web directory, defined in section 2.1 of this CP.

6.1.5 Key length

The key length of the CA Internal Certificates is 4096 bits.

6.1.6 Public Key Generation Parameters and Quality Verification

The public key of the internal certificates is encoded in accordance with RFC 5280 and RFC 3279.

6.1.7 Supported Key Usage (X.509 v3 KeyUsage Field)

The supported key uses for the internal certificates are given by the value of *Key Usage and Extended Key Usage* extensions. The contents of these extensions for each of internal certificate types can be consulted in section 7.1.2 of this document.

6.2 Private key protection and engineering control for modules

6.2.1 Standards for Cryptographic Modules

The modules used for the key creation used by CORPME TSP CAs comply with the FIPS 140-2 level 3 certification.

6.2.2 Multi – person control (K of N) of the private key

The external certificates private keys are not under multi-person control. The control of said private key falls entirely on subscriber.

6.2.3 Private Key Custody

The owners themselves carry out external certificate private keys custody.

6.2.4 Private Key Backup

In no case will the private signing external certificates keys be backed up to guarantee non-repudiation.

6.2.5 Archiving the Private Key

External certificates Private signing keys will never be archived to ensure non-repudiation.

6.2.6 Transferring the Private Key to/or from Cryptographic Module

In no case is it possible to transfer external certificates' private signing keys to ensure non-repudiation.

6.2.7 Storing Private Key in a Cryptographic Module

Private signing keys for external certificates are generated on cryptographic device at the time of certificate generation.

6.2.8 Method for activating the private key

The owner of the same can do Private Key activation by using your PIN.

6.2.9 Method for deactivating the private key

Not stipulated.

6.2.10 Private Key Destruction Method

Not stipulated.

6.2.11 Cryptographic Modules Classification

The cryptographic modules used meet the FIPS 140-2 level 3 standard.

6.3 Other aspects of Key Pair management

6.3.1 Public Key File

As specified in CORPME Certification Practice Statement (CPS).

6.3.2 Certificate operative periods and Key Pair usage period

The validity period of internal certificates is two (2) years from the time of certificate issuance, except for SSL certificates, which will be at the request of the Applicant between a minimum validity of one (1) year and a maximum validity Of five (5) years, as well as the certificates of registry procedures whose duration will be of (3) years.

6.4 Activation data

6.4.1 Generation and Installation of Activation Data

As specified in CORPME Certification Practice Statement (CPS).

6.4.2 Activation data protection

As specified in CORPME Certification Practice Statement (CPS).

6.4.3 Other aspects of activation data

As specified in CORPME Certification Practice Statement (CPS).

6.5 Computer Security Controls

6.5.1 Specific technical security requirements

As specified in CORPME Certification Practice Statement (CPS).

6.5.2 Computer security assessment

As specified in CORPME Certification Practice Statement (CPS).

6.6 Lifecycle security controls

6.6.1 System Development Controls

As specified in CORPME Certification Practice Statement (CPS).

6.6.2 Security Management Controls

As specified in CORPME Certification Practice Statement (CPS).

6.6.3 Lifecycle Security Controls

As specified in CORPME Certification Practice Statement (CPS).

6.7 Network Security Controls

As specified in CORPME Certification Practice Statement (CPS).

6.8 Time Stamping

As specified in CORPME Certification Practice Statement (CPS).

7 CERTIFICATES, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number

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

7.1.2 Certificate extensions

The extensions used in certificates are:

- *Subject Key Identifier*
- *Authority Key Identifier*
- *Certificate Policies*
- *Basic Constraints*
- *Key Usage*
- *Extended Key Usage*
- *Subject Alternative Name*
- *CRL Distribution Points*
- *Authority Information Access (AIA)*
- *EU Qualified Certificate Extensions (EU-qualified)*
    - *Qualified Certificate Statements*
    - *QCSyntax v2*
    - *EU Qualified Certificate Policy Identifier*

7.1.2.1 Registrar Qualified Certificate

These are the X.509 v3 certificate fields and extensions:

Field / Extension	Content	Critical	Observations
Version	Vv3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles,		All *DirectoryString* coded in UTF8. The attribute "C" (*countryName*) will be coded acording to "*ISO 3166-1-alpha-2 code elements"*, in *PrintableString*.

	CN=Autoridad de Certificación de los Registradores - AC Interna		
Validity	2 years		
Subject	As defined in section 3.1.1.1		All *DirectoryString* coded in UTF8. The attribute "C" (*countryName*) will be coded acording to "*ISO 3166-1-alpha-2 code elements"*, in *PrintableString*. The attribute *SerialNumber* will be coded in *PrintableString*.
Subject Public Key	Algorithm: RSA Encryption Length: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Function hash sha1 for the subject public key	NO	
Authority Key Identifier	Function hash sha1 for the AC public key issuer	NO	
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.1.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Personal Interno de los Registros, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Field coded in UTF8.
- Policy Identifier (EU Qualified Certificate)	QCP-natural-qscd (**0.4.0.194112.1.2**)		In compliance with the European standard 910/2014 and following the recommendations established by the ETSI standard.
Subject Alternative Name	**Rfc822Name** = *correo_registrador@registradores.org* **UPN** = UserID@Domain ➢ UPN OtherName OID is: "1.3.6.1.4.1.311.20.2.3" ➢ The value "UPN OtherName" must be coded in UTF8 **directoryName=** ➢ **1.3.6.1.4.1.17276.1.0.0.1**:*POSTAL ADDRESS* ➢ **1.3.6.1.4.1.17276.1.0.0.2**: *NAME* ➢ **1.3.6.1.4.1.17276.1.0.0.3**: *SURNAME1* ➢ **1.3.6.1.4.1.17276.1.0.0.4**: *SURNAME2* ➢ **1.3.6.1.4.1.17276.1.0.0.5**: *NIF* ➢ **1.3.6.1.4.1.17276.1.1.1.1**:*Registrar Status* ➢ All values must be coded in UTF8 ➢ Values specified in UPPERCASE must be in UPPERCASE	NO	The fields 1.3.6.1.4.1.311.20.2.3 (UPN) and 1.3.6.1.4.1.17276.1.0.0.1 (Postal Address) are optional. [RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:**	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.

	ldap://ldap.registradores.org/ CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20– %20Q2863012G, C=ES?certificateRevocationList?base ?objectclass=cRLDistributionPoint		
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Alternative Name (Access Location):** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Alternative Name (Access Location)** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
Key Usage	Digital Signature Non-Repudiation Key Agreement	YES	
Extended Key Usage	Client Authentication Secure Mail Smart Card Logon	NO	
Qualified Certificate Statements	QCCompliance (**0.4.0.1862.1.1**) QcEuRetentionPeriod (**0.4.0.1862.1.3**) = 15 years QCSSCD (**0.4.0.1862.1.4**) QCPSS (**0.4.0.1862.1.5**) = https://pki.registradores.org/normativa/en/tsp_information.htm QcType-esign (**0.4.0.1862.1.6.1**)	NO	In compliance with the European standard 910/2014 and following the recommendations established by the ETSI standard.
QCSyntax-v2	id-etsi-qcs-SemanticsId-Natural (**0.4.0.194121.1.1**)	NO	QcSemantics for physical person.
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	YES	

7.1.2.2 Internal Personnel Qualified Certificate

These are the X.509 v3 certificate fields and extensions:

Field / Extension	Content	Critical	Observations
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		All *DirectoryString* coded in UTF8. The attribute "C" (*countryName*) will be coded acording to "*ISO 3166-1-alpha-2 code elements*", in *PrintableString*.
Validity	2 years		Validity period Start date

Subject	As defined in section 3.1.1.2		All *DirectoryString* coded in UTF8. The attribute "C" (*countryName*) will be coded acording to "*ISO 3166-1-alpha-2 code elements"*, in *PrintableString*. The attribute *SerialNumber* will be coded in *PrintableString*.
Subject Public Key	Algorithm: RSA Encryption Length: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Function hash sha1 for the subject public key	NO	
Authority Key Identifier	Function hash sha1 for the AC public key issuer	NO	
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.2.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Personal Interno de los Registros, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Field coded in UTF8.
- Policy Identifier (EU Qualified Certificate)	QCP-natural-qscd (**0.4.0.194112.1.2**)		In compliance with the European standard 910/2014 and following the recommendations established by the ETSI standard.
Subject Alternative Name	**Rfc822Name** = *correo_corporativo@domain.com* **UPN** = UserID@Domain ➢ UPN OtherName OID es: "1.3.6.1.4.1.311.20.2.3" ➢ The value "UPN OtherName" must be coded in UTF8 **directoryName=** ➢ **1.3.6.1.4.1.17276.1.0.0.1**: *POSTAL ADDRESS* ➢ **1.3.6.1.4.1.17276.1.0.0.2**: *NAME* ➢ **1.3.6.1.4.1.17276.1.0.0.3**: *SURNAME1* ➢ **1.3.6.1.4.1.17276.1.0.0.4**: *SURNAME2* ➢ **1.3.6.1.4.1.17276.1.0.0.5**: *NIF* ➢ **1.3.6.1.4.1.17276.1.1.2.1**: *Subtype* ➢ **1.3.6.1.4.1.17276.1.1.2.2**: *ORGANIZATION* ➢ **1.3.6.1.4.1.17276.1.1.2.3**: *POSITION* ➢ All values must be coded in UTF8 ➢ Values specified in UPPERCASE must be in UPPERCASE	NO	The fields 1.3.6.1.4.1.311.20.2.3 (UPN) and 1.3.6.1.4.1.17276.1.0.0.1 (Postal Address) are optional. The field 1.3.6.1.4.1.17276.1.1.2.2 (Organization) is conditional. [RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:**	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.

	ldap://ldap.registradores.org/ CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20– %20Q2863012G, C=ES?certificateRevocationList?base ?objectclass=cRLDistributionPoint		
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Alternative Name (Access Location):** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Alternative Name (Access Location)** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
Key Usage	Digital Signature Non Repudiation Key Agreement	YES	
Extended Key Usage	Client Authentication Secure Mail Smart Card Logon	NO	
Qualified Certificate Statements	QCCompliance (**0.4.0.1862.1.1**) QcEuRetentionPeriod (**0.4.0.1862.1.3**) = 15 years QCSSCD (**0.4.0.1862.1.4**) QCPSS (**0.4.0.1862.1.5**) = https://pki.registradores.org/normativa/en/tsp_information.htm QcType-esign (**0.4.0.1862.1.6.1**)	NO	In compliance with the European standard 910/2014 and following the recommendations established by the ETSI standard.
QCSyntax-v2	id-etsi-qcs-SemanticsId-Natural (**0.4.0.194121.1.1**)	NO	QcSemantics for natural person.
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	YES	

7.1.2.3 Qualified Certificate of Legal Person Representative for Electronic Invoicing

These are the X.509 v3 certificate fields and extensions:

Field / Extension	Content	Critical	Observations
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		All *DirectoryString* coded in UTF8. The attribute "C" (*countryName*) will be coded acording to "*ISO 3166-1-alpha-2 code elements*", in *PrintableString*.
Validity	2 years		

Subject	As defined in section 3.1.1.3		All *DirectoryString* coded in UTF8. The attribute "C" (*countryName*) will be coded acording to "*ISO 3166-1-alpha-2 code elements"*, in *PrintableString*. The attribute *SerialNumber* will be coded in *PrintableString*.
Subject Public Key	Algorithm: RSA Encryption Length: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Function hash sha1 for the subject public key	NO	
Authority Key Identifier	Function hash sha1 for the AC public key issuer	NO	
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.4.1		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Representante de Entidad Jurídica para Facturación Electrónica, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Field coded in UTF8.
- Policy Identifier (EU Qualified Certificate)	QCP-natural-qscd (**0.4.0.194112.1.2**)		In compliance with the European standard 910/2014 and following the recommendations established by the ETSI standard.
Subject Alternative Name	**Rfc822Name** = *correo_representante@domain.com* **directoryName=** ➢ **1.3.6.1.4.1.17276.1.0.0.1**: *POSTAL ADDRESS* ➢ **1.3.6.1.4.1.17276.1.0.0.2**: *NAME* ➢ **1.3.6.1.4.1.17276.1.0.0.3**: *SURNAME1* ➢ **1.3.6.1.4.1.17276.1.0.0.4**: *SURNAME2* ➢ **1.3.6.1.4.1.17276.1.0.0.5**: *NIF* ➢ **1.3.6.1.4.1.17276.1.2.2.3**: *POSITION* ➢ All values must be coded in UTF8 ➢ Values specified in UPPERCASE must be in UPPERCASE	NO	The field 1.3.6.1.4.1.17276.1.0.0.1 (Postal Address) is optional. [RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20INTERNA,O=Colegio%20de%20Registradores%20–%20Q2863012G,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.

Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Alternative Name (Access Location):** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Alternative Name (Access Location)** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
Key Usage	Digital Signature Non Repudiation Key Agreement	SI	
Extended Key Usage	Client Authentication Secure Mail	NO	
Qualified Certificate Statements	QCCompliance (**0.4.0.1862.1.1**) QcEuRetentionPeriod (**0.4.0.1862.1.3**) = 15 years QCSSCD (**0.4.0.1862.1.4**) QCPSS (**0.4.0.1862.1.5**) = https://pki.registradores.org/normativa/en/tsp_information.htm QcType-esign (**0.4.0.1862.1.6.1**)	NO	In compliance with the European standard 910/2014 and following the recommendations established by the ETSI standard.
QCSyntax-v2	id-etsi-qcs-SemanticsId-Natural (**0.4.0.194121.1.1**)	NO	QcSemantics for natural person.
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	SI	

7.1.2.4 Non-Qualified Certificate for Registration Procedures

These are the X.509 v3 certificate fields and extensions:

Field / Extension	Content	Critical	Observations
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norma PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		Matches the subject field of the Internal Subordinate CA certificate. All DirectoryString encoded in UTF8. The "C" (*countryName*) attribute will be encoded according to "ISO 3166-1-alpha-2 code elements", in *PrintableString*.
Validity	3 years		
Subject	As defined in section 3.1.1.4		All DirectoryString encoded in UTF8. The "C" (*countryName*) attribute will be encoded according to "ISO 3166-1-alpha-2 code elements", in *PrintableString*.
Subject Public Key	Algorithm : RSA Encryption Length: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Function hash sha1 for the subject public key	NO	

Authority Key Identifier	Function hash sha1 for the AC public key issuer	NO	
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.3.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado No Cualificado para Procedimientos Registrales, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Field coded in UTF8.
Subject Alternative Name	**Rfc822Name** = *correo_responsable@domain.com* **directoryName =** ➢ **1.3.6.1.4.1.17276.1.0.0.1**: *POSTAL ADDRESS* ➢ **1.3.6.1.4.1.17276.1.1.6.1:** operador ➢ All values must be coded in UTF8 ➢ Values specified in UPPERCASE must be in UPPERCASE ➢	NO	[RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20–%20Q2863012G, C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Access Location:** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Access Location** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
Key Usage	Digital Signature Non Repudiation Key Agreement	YES	
Extended Key Usage	clientAuth serverAuth	NO	
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	YES	

7.1.2.5 Generic SSL Non-Qualified Certificate

These are the X.509 v3 certificate fields and extensions:

Field / Extension	Content	Critical	Observations
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norm PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores – AC Interna		Matches the subject field of the Internal Subordinate CA certificate. All DirectoryString encoded in UTF8. The "C" (*countryName*) attribute will be encoded according to "ISO 3166-1-alpha-2 code elements", in *PrintableString*
Validity	2 years		
Subject	As defined in section 3.1.1.5		All DirectoryString encoded in UTF8. The "C" (*countryName*) attribute will be encoded according to "ISO 3166-1-alpha-2 code elements", in *PrintableString*.
Subject Public Key	Algorithm: RSA Encryption Length: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Function hash sha1 for the subject public key	NO	
Authority Key Identifier	Function hash sha1 for the AC public key issuer	NO	
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.6.2		
-- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/ normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado No Cualificado de SSL Genérico, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		
Subject Alternative Name	**Rfc822Name** = *correo_responsable@domain.com* **DNSName =** *al menos el nombre DNS del CN así como otros nombres DNS*	NO	[RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities.

			Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20–%20Q2863012G, C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
8. Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Access Location:** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Access Location** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
Key Usage	Digital Signature Key Encipherment Key Agreement	YES	
Extended Key Usage	clientAuth serverAuth	NO	
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	YES	

7.1.3 Object identifiers (OID) of algorithms

Cryptographic algorithms Object Identifier (OID): 1.3.6.1.4.1.17276.0.1.0.1.0

7.1.4 Name format

External certificates contain the X.500 distinguished issuer name and certificate holder in the issuer name and subject name fields respectively

7.1.5 Name Restrictions

The name restrictions are described in section 3.1.1 of this document.

7.1.6 Certification Policy Object Identifier (OID)

The OIDs for this CP are as follows:

- Registrar Qualified Certificates: 1.3.6.1.4.1.17276.0.1.1.2
- Internal Personnel Qualified Certificates: 1.3.6.1.4.1.17276.0.1.2.2
- Qualified Certificates of Legal Person Representative for Electronic Invoicing: 1.3.6.1.4.1.17276.0.1.4.1
- Non-Qualified Certificates for Registration Procedures: 1.3.6.1.4.1.17276.0.1.3.2
- Generic SSL Non-Qualified Certificates: 1.3.6.1.4.1.17276.0.1.6.2

7.1.7 Using the extension "PolicyConstraints"

Not stipulated.

7.1.8 "Syntax of the "PolicyQualifier"

The *Certificate Policies* extension contents can be found in section 7.1.2 of this document.

7.1.9 Semantic processing for critical extension "Certificate Policy"

Not stipulated.

7.2 CRL Profile

7.2.1 Version Number

As specified in CORPME Certification Practice Statement (CPS).

7.2.2 CRL and extensions

As specified in CORPME Certification Practice Statement (CPS).

7.3 OCSP Profile

7.3.1 Version Number(s)

As specified in CORPME Certification Practice Statement (CPS).

7.3.2 OCSP Extension

As specified in CORPME Certification Practice Statement (CPS).

8 COMPLIANCE AUDITS AND OTHER CONTOLS

8.1 Frequency or circumstances of controls for each Authority

As specified in CORPME Certification Practice Statement (CPS).

8.2 Auditor Identification / Qualification

As specified in CORPME Certification Practice Statement (CPS).

8.3 Relationship between auditor and Audited Authority

As specified in CORPME Certification Practice Statement (CPS).

8.4 Aspects covered by controls

As specified in CORPME Certification Practice Statement (CPS)..

8.5 Actions to be taken because of deficiencies detection

As specified in CORPME Certification Practice Statement (CPS).

8.6 Communication of results

As specified in CORPME Certification Practice Statement (CPS).

9 OTHER LEGAL AND ACTIVITY ISSUES

9.1 Rates

9.1.1 Certificate or renewal rates

As specified in CORPME Certification Practice Statement (CPS).

9.1.2 Certificate access fees

As specified in CORPME Certification Practice Statement (CPS).

9.1.3 Access fees to the information status or revocation

As specified in CORPME Certification Practice Statement (CPS).

9.1.4 Other service rates

As specified in CORPME Certification Practice Statement (CPS).

9.1.5 Refund Policy

As specified in CORPME Certification Practice Statement (CPS).

9.2 Economic Responsibilities

As specified in CORPME Certification Practice Statement (CPS).

9.3 Confidentiality of information

As specified in CORPME Certification Practice Statement (CPS).

9.3.1 Confidential information scopes

As specified in CORPME Certification Practice Statement (CPS).

9.3.2 Non confidential information

As specified in CORPME Certification Practice Statement (CPS).

9.3.3 Professional Secrecy Duty

As specified in CORPME Certification Practice Statement (CPS).

9.4 Personal Information Protection

As specified in CORPME Certification Practice Statement (CPS).

9.5 Intellectual Property Rights

As specified in CORPME Certification Practice Statement (CPS).

9.6 Representation and Warranties

9.6.1 CA's Obligations

As specified in CORPME Certification Practice Statement (CPS).

9.6.2 RA's Obligations

As specified in CORPME Certification Practice Statement (CPS).

9.6.3 License holders obligation

As specified in CORPME Certification Practice Statement (CPS).

9.6.4 Obligations of third parties who trust or accept certificates

As specified in CORPME Certification Practice Statement (CPS).

9.6.5 Other participant obligations

As specified in CORPME Certification Practice Statement (CPS).

9.7 Disclaimer

As specified in CORPME Certification Practice Statement (CPS).

9.8 Limitations of Responsibilities

As specified in CORPME Certification Practice Statement (CPS).

9.9 Indemnification

As specified in CORPME Certification Practice Statement (CPS).

9.10 Validity Period

9.10.1 Time Limit

This CP will come into effect from the moment of its publication in the CORPME's web directory and will be in force as long as it is not expressly waived by the issuance of a new version.

9.10.2 CP Replacement and repeal

This CP will be replaced by a new version regardless of the significance of the changes made in it, so that it will always be fully applicable.

When the CP is revoked, it will be removed from the CORPME web directory, although it will be kept for fifteen (15) years.

9.10.3 Completion Effects

The obligations and restrictions established by this CP, in reference to audits, confidential information, obligations and responsibilities of the CORPME TSP, born under its validity, will survive after its replacement or repeal by a new version in everything in which it does not oppose this one.

9.11 Individual notifications and communications with participants

As specified in CORPME Certification Practice Statement (CPS).

9.12 Specifications Changes Procedures

9.12.1 Changes Procedures

As specified in CORPME Certification Practice Statement (CPS).

9.12.2 Circumstances in which OID must be changed

As specified in CORPME Certification Practice Statement (CPS).

9.13 Claims

As specified in CORPME Certification Practice Statement (CPS).

9.14 Applicable regulations

As specified in CORPME Certification Practice Statement (CPS).

9.14.1 Compliance with applicable regulations

As specified in CORPME Certification Practice Statement (CPS).

9.15 Various Stipulations

9.15.1 Full Acceptance Clause

As specified in CORPME Certification Practice Statement (CPS).

9.15.2 Independence

In the event that one or more stipulations of this CP are or become invalid, or legally unenforceable, shall be understood as not being established, unless such provisions were essential so that excluding them from the CP would not be effective.

9.15.3 Judicial resolution

As specified in CORPME Certification Practice Statement (CPS).

9.16 Other Stipulations

Not stipulated.