Registradores DE ESPAÑA

EXTERNAL CERTIFICATION POLICIES

Trust Service Provider

Information Systems Service
May 29th, 2017

Registradores DE ESPAÑA
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 External Certification Policies	File/s name: REG-PKI-DPC03v.1.0.3 External Certification Policies.pdf
Code: REG-PKI-DPC03	Logical Support: MS-DOCX y PDF
Date: 29/05/2017	Physical location: http://pki.registradores.org/normativa/index.htm
Version: 1.0.3	

CHANGE RETENTION		
Version	**Date**	**Reason for change**
0.0.2	17/06/2016	Review and submission for document approval
1.0.0	20/06/2016	Document approval
1.0.1	19/09/2016	Added "IDCES" to Representative with and without pers. Legal. Modifications LFE / 2016/0071
1.0.2	23/11/2016	Modification (2) LFE/2016/0071
1.0.3	29/05/2017	Adaptation to eIDAS Regulation

DOCUMENT DISTRIBUTION	
Name	**Area**
Public	Public / Internet

DOCUMENT CONTROL			
DRAFTED	**INSPECTED**	**APPROVED**	**ADMITTED**
PwC	Óscar Yagüe	Raúl Avedillo	Luis Alberto Lahoz
29/05/2017	29/05/2017	29/05/2017	29/05/2017

INDEX

1 INTRODUCTION

1.1 Overview

The Public Corporation of Land and Business Registers of Spain, Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles 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 TSP Rules of Procedure.

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

1.2 CPS Document and Identification name

This document is called *CORPME EXTERNAL CERTIFICATION POLICIES.*

Document Identification:

Document´s name	CORPME External Certification Policies
Document's version	1.0.3
Document's status	Version
Date of Issue	29/05/2017
Date of expiration	No applicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.2.0.1.0.3
CP location	http://pki.registradores.org/normativa/index.htm
Related CPS	CORPME Certification Practice Statement

1.3 Participants in the Public Key Infrastructure (PKI) of the Trust Service Provider of the Colegio de Registradores

1.3.1 Trust Service Provider (TSP)

It is the entity responsible for the issuance, under the hierarchy of its root certificate, of the digital certificates destined to end entities, as well as the life cycle management of the digital certificates.

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

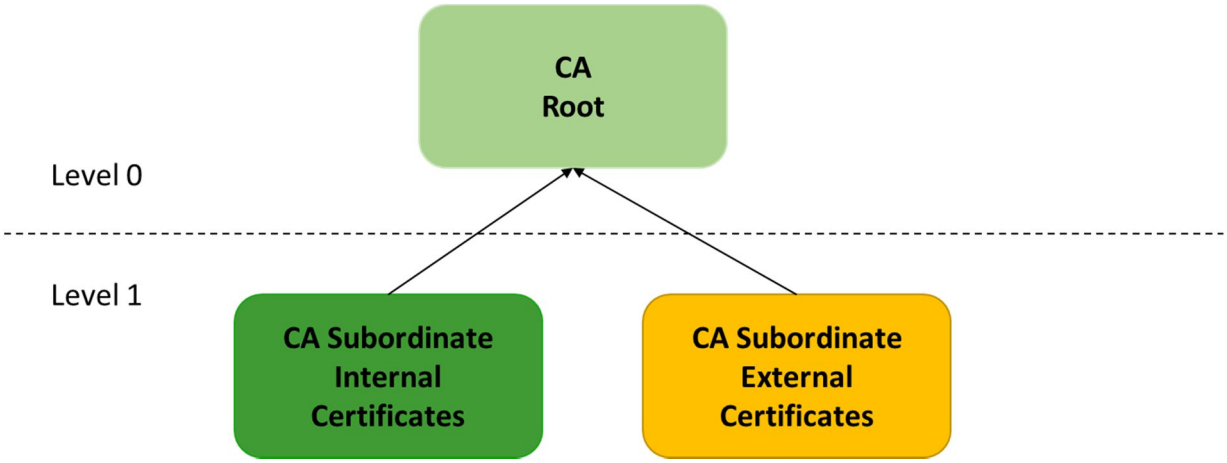
Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España

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

In CORPME, in addition to being a provider (TSP), the CA (Certification Authority) is in charge of carrying out its activity in accordance with the legislation in force in this area, notably ley 59/2003, de 20 de diciembre de Firma Electrónica and The EU 910/2014 regulation of electronic identification and services of trust. Certification services are, in any case, applied in accordance with the principle of non-discrimination.

The TSP has an Information Security Management System for all CORPME certification services, as well as a Quality Management System for the Time Stamping Authority (TSA) service.

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 said 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 analysing 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 TSP 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
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 Subordinated 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 subordinated 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
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. Internal Personnel Qualified Certificate. Qualified Certificate of Legal Entity Representative for Electronic Invoicing. Non-Qualified Certificate for Registration Procedures. Generic SSL Non-Qualified Certificate.

The most relevant information of the subordinated 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
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. Legal Person Representative Qualified Certificate. Entity without Legal Personality Representative Qualified Certificate. Administrative Position Qualified Certificate. Local Administration Qualified Certificate. Professional Qualified Certificate.

1.3.5 Registration Authority

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

- Business Records.
- Decanatos.
- Property records.
- 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, 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 titular, interim or accidental registrar, except;

- The Decanatos, 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 Board of Governors, 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://www.registradores.org/scr/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 TSP 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 legal 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 trust in CORPME certificates.

1.3.8.1 Applicant

When a person interested in obtaining a certificate issued by CORPME, completes the appointment request form of **https://www.registradores.org/scr/agenda**, he / she acquires the status of 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 Legal Person Representative Qualified Certificates, the natural person who, by virtue of a power of attorney registered in the Business Registry bears the representation of a juridical person, including the information of the latter in the certificate.
- In case of the issuance of Entity without Legal Person Representative Qualified Certificates, 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 Legal Person Representatives Qualified Certificates 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*), and G (*Given Name*), S (*Surname*) *Subject* of the certificate. Subscriber identification data may also be included, depending on the type of certificate, with format RFC6854 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 section Description of the *Distinguished Name* field of the digital certificate.

1.3.8.3 Third parties that trusts 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.

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, Mercantiles y de Bienes Muebles 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: Royal Observatory of the Spanish Navy.

SSI: Information Systems Service of the CORPME.

SSL: Secure Sockets Layer.

TSA: Time Stamp Authority (Time Stamping Authority).

TSP: Trust Service Provider.

TST: Time Stamp Token (Token Time Stamping).

TSU: Time Stamp 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, so that, 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, which contains all the CRLs issued by the Trust Service Provider, whose expiration period has not yet expired, including the date and Time at which the 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 that implements 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, will have the published ARL, and published CRLs, which follow 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 at the intervals 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 thereto. 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 that want it. CORPME will have the necessary security measures to prevent unauthorized manipulation of these documents. They will also be digitally signed by a certificate issued by CORPME to guarantee its integrity.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Names

3.1.1 Name Types

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

3.1.1.1 Personal Qualified Certificate

The structure of the certificate, referring to the certificate´s subject extension, is the one described in the following table:

Field	Value	Description
C	ES	Country
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Required by ETSI EN 319 412-2
SN	*APELLIDOS*	**surname.** Required by ETSI EN 319 412-2
G	*NOMBRE*	**givenName.** Required by ETSI EN 319 412-2
CN	NOMBRE *nombre apellidos*– NIF *nif*	All this information must go in UPPERCASE

3.1.1.2 Legal Person Representative Qualified Certificate

The structure of the certificate, referring to the certificate´s subject extension, is the one described in the following table:

Field	Value	Description
C	ES	Country
description	Reg: *XXX* /Hoja: *XXX* /Tomo:*XXX* /Sección:*XXX* /Libro:*XXX* /Folio:*XXX* /Fecha: *dd-mm-aaaa* /Inscripción: *XXX*	Public document codification that accredits signer o registry data faculties
organizationIdentifier	VATES-*nif*	Entity CIF (@firma and Required by ETSI 319 412-2)

O	*Razón social*	Organization for @firma (Required by ETSI 319 412-2)
1.3.6.1.4.1.18838.1.1	*Dni / nie / pasaporte del Representante*	OID AEAT
SERIALNUMBER	IDCES-*Dni / nie / pasaporte*	**serialNumber.** Required by ETSI EN 319 412-2
SN	*APELLIDOS*	**surname.** Required by ETSI EN 319 412-2
G	*NOMBRE*	**givenName.** Required by ETSI EN 319 412-2
CN	*DNI NOMBRE APELLIDOS*	All this information must go in UPPERCASE The field has a maximum length of 64 characters in accordance with RFC 5280.

3.1.1.3 Entity without Legal Personality Representative Qualified Certificate

The structure of the certificate, referring to the certificate´s subject extension, is the one described in the following table:

Field	Value	Description
C	ES	Country
description	*CVE*	Public document Codification that accredits signer or the registry data faculties (CVE-BOE)
organizationIdentifier	NTRES-*Código de la Entidad Representada*	CIF (Required by @firma y ETSI 319 412-2)
O	*Denominación de la Entidad Representada*	Organization for @firma (Required by ETSI 319 412-2)
1.3.6.1.4.1.18838.1.1	*Dni / nie / pasaporte del Representante*	OID AEAT
SERIALNUMBER	IDCES-*Dni / nie / pasaporte*	**serialNumber.** Required by ETSI EN 319 412-2
SN	*APELLIDOS*	**surname.** Required by ETSI EN 319 412-2
G	*NOMBRE*	**givenName.** Required by ETSI EN 319 412-2

CN	*DNI NOMBRE APELLIDOS*	All this information must go in UPPERCASE The field has a maximum length of 64 characters in accordance with RFC 5280.

3.1.1.4 Administrative Position Qualified Certificate

The structure of the certificate, referring to the certificate´s subject extension, is the one described in the following table:

Field	Value	Description
C	ES	Country
organizationIdentifier	*NIF de la Administración*	Administration NIF
O	*Administración Representada*	Organization
OU	*Órgano Administrativo*	
OU	*Unidad Local*	
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Required by ETSI EN 319 412-2
SN	*APELLIDOS*	**surname.** Required by ETSI EN 319 412-2
G	*NOMBRE*	**givenName.** Required by ETSI EN 319 412-2
CN	*NOMBRE APELLIDOS* – DNI *nif*	All this information must go in UPPERCASE Subscriber Nif

3.1.1.5 Local Administration Qualified Certificate

The structure of the certificate, referring to the certificate´s subject extension, is the one described in the following table:

Field	Value	Description
C	ES	Country
organizationIdentifier	*NIF de la Administración*	Administration NIF (LAESCP)
O	*Administración Representada (Unidad Local)*	Organization

OU	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO	Required by RD 668/2015
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Required by ETSI EN 319 412-2
SN	*APELLIDOS*	**surname.** Required by ETSI EN 319 412-2
G	*NOMBRE*	**givenName.** Required by ETSI EN 319 412-2
CN	*NOMBRE APELLIDOS* – DNI *nif*	All this information must go in UPPERCASE

3.1.1.6 Professional Qualified Certificate

The structure of the certificate, referring to the certificate´s subject extension, is the one described in the following table:

Field	Value	Description
C	ES	Country
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Required by ETSI EN 319 412-2
SN	*APELLIDOS*	**surname.** Required by ETSI EN 319 412-2
G	*NOMBRE*	**givenName.** Required by ETSI EN 319 412-2
CN	NOMBRE *nombre apellidos* – NIF *nif*	All this information must go in UPPERCASE

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 it issues is ISO / IEC 9595 (X.500) Distinguished Name (DN).

3.1.4 Uniqueness of names

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

- For Personal Qualified Certificates, name use (composed of the surnames and name), and NIF (composed of the NIF, NIE, passport or other) in the CN guarantees the uniqueness of the same.
- For Legal Person Representative Qualified Certificates, entity use (composed of the company name), NIF, name (composed of the surnames and name), and NIF (composed of the NIF, NIE, passport or another) in CN guarantees the uniqueness of the same.
- For Entity without Legal Personality Representative Qualified Certificates, entity use (composed of the company name), official univoc Identifier, name (composed of surnames and name), and NIF (composed of the NIF, NIE, passport or other) in the CN guarantees the uniqueness of the same.
- For Administrative Position Qualified Certificates, name use (composed of surnames and name), and of NIF (composed of NIF, NIE, passport or other) in CN guarantees the uniqueness of the same.
- For Local Administration Qualified Certificates, name use (composed of surnames and name), and NIF (composed of NIF, NIE, passport or other) in CN guarantees the uniqueness of the same.
- For Professional Qualified Certificates, name use (composed of surnames and name), and 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 resolved 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 keys of external certificates:

- Personal Qualified Certification.
- Legal Person Representative Qualified Certificate.
- Entity without Legal Personality Representative Qualified Certificate.
- Administrative Position Qualified Certificate.
- Local Administration Qualified Certificate.
- Professional Qualified Certificate.

will be generated by the Applicant's secure cryptographic device being 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 certificate holder will carry out the order of generation of the keys and the introduction of passwords in the cryptographic device personally.

3.2.2 Authentication of Identity for Legal Persons

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

Foreign Applicants for CORPME certificates, must appear, with their foreign identification number (NIE), their passport, their residence card or any other legal document of identification.

Besides the applicant identification by checking the above mentioned documentation, the corresponding Registry Officer must request the documentation proving the certifiable attribute depending on the type of certificate, except for Legal Person Qualified Certificates where the Registry Officer may obtain a note proving the validity and data of the position in the corresponding Business Registry, either through the FLEI service or through a note issued by the Business Registry management system (if the Processing Unit is placed within a Business Registry.

Regarding Entity without Legal Personality Representative Qualified Certificates, the Registry Officer must verify that the CVE of Boletín Oficial del Estado (BOE) is accessible and reflects the applicant's appointment.

3.2.3 Authentication of Identity for Legal Persons

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

3.2.3.1 Personal Qualified Certificate

- Subscriber's name and surname.
- Subscriber' Identity document (DNI / NIF / Passport / NIE).
- Email.
- Phone number.
- Postal address (optional).

3.2.3.2 Legal Person Representative Qualified Certificate

- Subscriber's name and surname.
- Subscriber' Identity document (DNI / NIF / Passport / NIE).
- Email.
- Phone number.
- Postal address (optional).
- Business name.
- NIF of the Represented Entity.
- Position or empowerment.
    - Documentary evidence that reflects the validity of the corresponding position or empowerment (this document is also used to provide information regarding registration data). In case of not being provided, the staff of the Processing Unit will obtain it by its means, either through the FLEI service (Reference File of Registered Companies) or through the note issued by the Business Registry management system (in case of a Processing Unit located in a Business Registry).
- Registration data.

- Documentary evidence that reflects the inscription in the Business Registry: LEI Code (optional), Registry, Sheet, Volume, Section, Book, Page, Registration and Registration Date (this document is also used to provide information regarding position or empowerment). In case of not being provided, the staff of the Processing Unit will obtain it by its means, either through the FLEI service (Reference File of Registered Companies) or through the note issued by the Business Registry management system (in case of a Processing Unit located in a Business Registry).

3.2.3.3 Entity without Legal Personality Representative Qualified Certificate

- Subscriber's name and surname.
- Subscriber' Identity document (DNI / NIF / Passport / NIE).
- CVE of the Official Bulletin (BOE) where the representation or ownership over the entity is published.
- Email.
- Phone number.
- Postal address (optional).
- Represented entity name.
- Represented entity code.

3.2.3.4 Administrative Position Qualified Certificate

- Subscriber's name and surname.
- Subscriber' Identity document (DNI / NIF / Passport / NIE).
- Email.
- Phone number
- Postal address (optional).
- Administrative position he / she holds, corresponding to his/her category.
  - Certificate confirming the validity of the position held.
- Name of the Represented Administration.
- NIF of the Represented Administration.
- Administrative body represented.
- Name of the Local Unit.

3.2.3.5 Local Administration Qualified Certificate

- Subscriber's name and surname.
- Subscriber's Identity document (DNI / NIF / Passport / NIE).
- Email.
- Phone number.
- Postal address (optional).
- Administrative position he / she holds, corresponding to his/her category.

- Certificate confirming the validity of the position held.
- NIF of the Local Administration.
- Province of Local Administration.
- Name of the Local Unit.

3.2.3.6 Professional Qualified Certificate

- Subscriber's name and surname.
- Subscriber's Identity document (DNI / NIF / National Passport).
- Email.
- Phone number.
- Postal address (optional).
- Profession, understood as the Professional Collective to which the Applicant for the certificate is attached.
    - Certificate confirming the corresponding profession, issued by a Professional association.

3.2.3.7 Authentication of Device Identity

Not stipulated.

3.2.4 Information not verified about the Applicant

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

3.2.5 Representation powers verification

Besides the Applicant identification by checking the above mentioned documentation, the corresponding Registry Officer must request the documentation proving the certifiable attribute depending on the type of certificate, except for Legal Person Representative Qualified Certificates where the Registry Officer may obtain a note proving the validity and data of the position in the corresponding Business Registry. This could be done either through the FLEI service or through a note issued by the Business Registry management system (if the Processing Unit is placed within a Business Registry).

The Processing Unit will verify the equivalence of the certification with the terms in which the certificate is written up, 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.

3.2.6 Criteria for operating with external CAs

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

3.3 Identification and authentication for renewal requests

The certificates holders' identification and authentication for the renewal requests for any reason, which are specified in section 4.7 of this document.

3.4 Identification and authentication for revocation requests

The certificates holders' identification and authentication for the revocation requests for any reason, which are specified in section 4.9 of this document.

4 OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF CERTIFICATES

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 Personal Qualified Certificate

The request for this type of certificate may be made by any person of legal age.

The request process requires a prior appointment. In these cases, as a preliminary step to obtain the certificate, the Applicant connects to the website https://www.registradores.org/scr/agenda. In case of not being registered it is mandatory to proceed with the registration. Once registered, an online form must be completed with the necessary information (day and time in the chosen Processing Unit) for the issuance of the certificate, from which the fields of the certificate will be filled in and the license to use the certificate will be generated.

Since the certificate license must be signed by the Registry Officer in charge of the Processing Unit, it is imperative that the personal appearance of the Applicant coincides with the presence of the Registrar in the Processing Unit, so the Applicant must select day and time, among those available and previously authorized by the Officer. Once the date and time have been set, the Applicant will receive by e-mail a receipt of the arranged appointment.

4.1.1.2 Legal Person Representative Qualified Certificate

The request for this type of certificate may be made by the positions of entities registered in the Business Registers.

The request process requires a prior appointment. In these cases, as a preliminary step to obtain the certificate, the Applicant should connect to the website https://www.registradores.org/scr/agenda. In case of not being registered it is mandatory to proceed with the registration. Once registered, an online form must be completed with the necessary information (day and time in the chosen Processing Unit) for the issuance of the certificate, from which the fields of the certificate will be filled in and the license to use the certificate will be generated.

Since the certificate license must be signed by the Registry Officer in charge of the Processing Unit, it is imperative that the personal appearance of the Applicant coincides with the presence of the Registrar in the Processing Unit, so the Applicant must select day and time, among those available and previously authorized by the Officer. Once the date and time have been set, the Applicant will receive by e-mail a receipt of the arranged appointment.

4.1.1.3 Entity without Legal Personality Representative Qualified Certificate

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

The request process does not require a prior appointment. In these cases, as a preliminary step to obtain the certificate, the Applicant should connect to the website https://www.registradores.org/scr/agenda. In case of not being registered it is mandatory to proceed with the registration. Once registered, an online form must be completed with the necessary information (day and time in the chosen Processing Unit) for the issuance of the certificate, from which the fields of the certificate will be filled in and the license to use the certificate will be generated.

Since the certificate license must be signed by the Registry Officer in charge of the Processing Unit, it is imperative that the personal appearance of the Applicant coincides with the presence of the Registrar in the Processing Unit, so the Applicant must select day and time, among those available and previously authorized by the Officer. Once the date and time have been set, the Applicant will receive by e-mail a receipt of the arranged appointment.

4.1.1.4 Administrative Position Qualified Certificate

The request for this type of certificate may be made by the positions of the public administration.

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.

4.1.1.5 Local Administration Qualified Certificate

The request for this type of certificate may be made by the personnel assigned to the local administration.

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.

4.1.1.6 Professional Qualified Certificate

The request for this type of certificate may be made by the personnel belonging to a professional association with an agreement with the provider.

The request process requires a prior appointment. In these cases, as a preliminary step to obtain the certificate, the Applicant connects to the website https://www.registradores.org/scr/agenda. In case of not being registered it is mandatory to proceed with the registration. Once registered, an online form must be completed with the necessary information (day and time in the chosen Processing Unit) for the issuance of the certificate, from which the fields of the certificate will be filled in and the license to use the certificate will be generated.

Since the certificate license must be signed by the Registry Officer in charge of the Processing Unit, it is imperative that the personal appearance of the Applicant coincides with the presence of the Registrar in the Processing Unit, so the Applicant must select day and time, among those available and previously authorized by the Officer. Once the date and time have been set, the Applicant will receive by e-mail a receipt of the arranged appointment.

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

In the requests for certificates that include interested party email, the CA will send notifying certificate issuance Applicant an email. This email is for information only. This notice applies to the following certificates:

- Personal Qualified Certificate.
- Legal Person Representative Qualified Certificate.
- Entity without Legal Personality Representative Qualified Certificate.
- Administrative Position Qualified Certificate.
- Local Administration Qualified Certificate.
- Professional Qualified Certificate.

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

4.5.1 Use of the private key and certificate by the holder

The Applicant must sign license to use certificate, accepting the same and the present CP. The license will necessarily include the following contents:

- **The personal data of the holder:** name and surname, telephone number and e-mail address.
- **A statement by the holder that,** if applicable, it states that it has received the cryptographic device containing private key and certificate and in which it undertakes to use it in accordance with the provisions of the CPS, and in the present CP.
- **The consent of the Applicant** for the transfer of their personal data to CORPME to extent that they are necessary for it to provide certification services. These data will be kept confidential in CORPME, and will never be transferred to third parties.

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 new 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

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 issuance of modified certificate to 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 the 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

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 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 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, are always generated during requestor appearance in the Processing Unit and with his personal intervention in process of assigning keys. The generation is done in any case within a cryptographic device with a level of security certified as: FIPS 140-1 level 2, or higher, CC EAL4 + or another with similar characteristics.

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

The public key of public officer certificates is generated in cryptographic device of holder at the issuing post, the RA being responsible for delivering the public key to the CA.

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 CORPME web directory, defined in section 2.1 of this CP.

6.1.5 Key length

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

6.1.6 Public Key Generation Parameters and Quality Verification

The external certificates public key is encoded in accordance with RFC6818.

6.1.7 Supported Key Usage (field KeyUsage de X.509 v3)

The supported external certificate key uses are given by the value of the *Key Usage* and *Extended Key Usage extensions*. The contents of these extensions for each of external 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 Private Key Multi – person control (K of N)

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 POther 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 external certificates period of validity is two (2) years from the time of issue of the same.

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 external 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 generically in certificates are: ¬

- *Subject Key Identifier*
- *Certificate Policies*
- *Basic Constraints*
- *Key Usage*
- *Thumbprint algorithm*
- *Thumbprint*
- *Subject Alternative Names*
- *CRL Distribution Points*
- *EU Qualified Certificate Extensions (EU-qualified)*
    - *Qualified Certificate Statements*
    - *QCSyntax v2*
    - *EU Qualified Certificate Policy Identifier*

7.1.2.1 Personal Qualified Certificate

Below is a breakdown of the most significant X.509 v3 certificate extensions:

Field	Proposed content	Review	Observations
Version	V3		
Serial number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles,		

	CN=Autoridad de Certificación de los Registradores – AC Externa		
Valid from			Validity period Start date
Valid to			End date of the validity period (2 years from the start of validity)
Subject			
Subject Public Key Info	Algorithm: RSA Encryption Length: 2048 bits		
Subject Key Identifier			
Authority Key Identifier			
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1. 17276.0.2.1.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado Personal, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		
- 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_personal@domain.com **1.3.6.1.4.1.17276.1.0.0.1**: *Dirección Postal* **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*	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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20EXTERNA,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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) QcPDS (**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	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.2 Legal Person Representative Qualified Certificate

Below is a breakdown of the most significant X.509 v3 certificate extensions:

Field	Proposed content	Review	Observations
Version	V3		
Serial number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		
Valid from			Validity period Start date
Valid to			End date of the validity period (2 years from the start of validity)

Subject			
Subject Public Key Info	Algorithm: RSA Encryption Length: 2048 bits		
Subject Key Identifier			
Authority Key Identifier			
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.2.2.2		
- 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, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		
- 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
- Policy Identifier	2.16.724.1.3.5.8		Legal Person Representative Qualified Certificate by the Ministry of Finance
Subject Alternative Name	**Rfc822Name =** correo_representante@domain.com **1.3.6.1.4.1.17276.1.0.0.1**: *Dirección Postal* **1.3.6.1.4.1.17276.1.0.0.2** *Nombre* **1.3.6.1.4.1.17276.1.0.0.3** *Apellido1* **1.3.6.1.4.1.17276.1.0.0.4** *Apellido2* **1.3.6.1.4.1.17276.1.0.0.5** *NIF* **1.3.6.1.4.1.17276.1.2.2.3**: *Cargo* **1.3.6.1.4.1.17276.1.2.2.4**: *Datos de Inscripción: Código LEI* **1.3.6.1.4.1.17276.1.2.2.5**: *Código Registro* **1.3.6.1.4.1.17276.1.2.2.6**: *Hoja* **1.3.6.1.4.1.17276.1.2.2.7**: *Tomo* **1.3.6.1.4.1.17276.1.2.2.8**: *Sección* **1.3.6.1.4.1.17276.1.2.2.9**: *Libro* **1.3.6.1.4.1.17276.1.2.2.10**: *Folio* **1.3.6.1.4.1.17276.1.2.2.11**: *Inscripción*	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_ext_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%20EXTERNA, 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 Externa): http://pki.registradores.org/certificados/a c_ext_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	
Enhanced 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**) QcPDS (**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	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.3 Entity without Legal Personality Representative Qualified Certificate

Below is a breakdown of the most significant X.509 v3 certificate extensions:

Field	Proposed content	Review	Observations
Version	V3		
Serial number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		

Valid from			Validity period Start date
Valid to			End date of the validity period (2 years from the start of validity)
Subject			
Subject Public Key Info	Algorithm: RSA Encryption Length: 2048 bits		
Subject Key Identifier			
Authority Key Identifier			
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.2.6.1		
- 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 sin Personalidad Jurídica, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		
- 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
- Policy Identifier	2.16.724.1.3.5.9		Entity without Legal Personality Representative Qualified Certificate by the Ministry of Finance.
Subject Alternative Name	**Rfc822Name** = correo_representante@domain.com **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* **1.3.6.1.4.1.17276.1.2.6.1**: *Position*	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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20EXTERNA,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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) QcPDS (**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	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.4 Administrative Position Qualified Certificate

Below is a breakdown of the most significant X.509 v3 certificate extensions:

Field	Proposed content	Review	Observations
Version	V3		
Serial number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		
Valid from			Validity period Start date
Valid to			End date of the validity period (2 years from the start of validity)
Subject			

Subject Public Key Info	Algorithm: RSA Encryption Length: 2048 bits		
Subject Key Identifier			
Authority Key Identifier			
Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1. 17276.0.2.3.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Cargo Administrativo, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		
- 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_cargo@domain.com **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** *Sruname1* **1.3.6.1.4.1.17276.1.0.0.4** *Surname2* **1.3.6.1.4.1.17276.1.0.0.5** *NIF* **1.3.6.1.4.1.17276.1.2.3.1**: *Administrative position* **1.3.6.1.4.1.17276.1.2.3.2**: *Administration* **1.3.6.1.4.1.17276.1.2.3.3**: *Administrative Body Represented* **1.3.6.1.4.1.17276.1.2.3.4**: *Local Unit*	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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20EXTERNA,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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) QcPDS (**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	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.5 Local Administration Qualified Certificate

Below is a breakdown of the most significant X.509 v3 certificate extensions:

Field	Proposed content	Review	Observations
Version	V3		
Serial number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		
Valid from			Validity period Start date
Valid to			End date of the validity period (2 years from the start of validity)
Subject			
Subject Public Key Info	Algorithm: RSA Encryption Length: 2048 bits		
Subject Key Identifier			
Authority Key Identifier			

Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1. 17276.0.2.4.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Administración Local, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		
- 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_cargo@domain.com **1.3.6.1.4.1.17276.1.2.4.1**: *Local Position* **1.3.6.1.4.1.17276.1.2.4.2**: *Local Administration Province* **1.3.6.1.4.1.17276.1.2.4.3**: *Local Unit* **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* **2.16.724.1.3.5.7.1.1:** PUBLIC EMPLOYEE ELECTRONIC CERTIFICATE **2.16.724.1.3.5.7.1.2:** *Owner Entity* **2.16.724.1.3.5.7.1.3:** *Owner Entity NIF* **2.16.724.1.3.5.7.1.4:** *Certificate Holder DNI* **2.16.724.1.3.5.7.1.6:** *Name* **2.16.724.1.3.5.7.1.7:** *Surname1* **2.16.724.1.3.5.7.1.8:** *Surname2*	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. Required by RD 668/2015 (LAESCP)
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20EXTERNA,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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) QcPDS (**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	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.6 Professional Qualified Certificate

Below is a breakdown of the most significant X.509 v3 certificate extensions:

Field	Proposed content	Review	Observations
Version	V3		
Serial number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Standard PKCS#1 v2.1 y RFC 3447.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		
Valid from			Validity period Start date
Valid to			End date of the validity period (2 years from the start of validity)
Subject			
Subject Public Key Info	Algorithm: RSA Encryption Length: 2048 bits		
Subject Key Identifier			
Authority Key Identifier			

Certificate Policies	It will be used	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.2.5.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Profesional, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		
- 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_profesional@domain.com **1.3.6.1.4.1.17276.1.2.5.1**: *Professional group which certificate holder is attached* **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*	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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20EXTERNA,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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) QcPDS (**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	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.3 Object identifiers (OID) of algorithms

Cryptographic algorithm object identifiers (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:

- Personal Qualified Certificates: 1.3.6.1.4.1.17276.0.2.1.2
- Legal Person Representative Qualified Certificates: 1.3.6.1.4.1.17276.0.2.2.2
- Entity without Legal Personality Representative Qualified Certificates: 1.3.6.1.4.1.17276.0.2.6.1
- Administrative Position Qualified Certificates: 1.3.6.1.4.1.17276.0.2.3.2
- Local Administration Qualified Certificates: 1.3.6.1.4.1.17276.0.2.4.2
- Professional Qualified Certificates: 1.3.6.1.4.1.17276.0.2.5.2

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) del CORPME.

7.2.2 CRL and extensions

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) del CORPME.

7.3 OCSP Profile

7.3.1 Version Number(s)

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) del CORPME.

7.3.2 OCSP Extension

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) del CORPME.

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 o 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 Rates for Access to state of revocation information

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, 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.