Registradores DE ESPAÑA

CERTIFICATION PRACTICE STATEMENT

Trust Service Provider

Information Systems Service
May 29th, 2017

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

DOCUMENTAL CONTROL

DOCUMENT / FILE	
Title: Certification Practice Statement	File/s name: REG-PKI-CPS01v.1.0.4 Certification Practice Statement .pdf
Code: REG-PKI-CPS01	Logical Support: MS-DOCX y PDF
Date: 29/05/2017	Physical location: http://pki.registradores.org/normativa/index.htm
Version: 1.0.4	

DOCUMENT VERSION CONTROL		
Version	**Date**	**Reason for change**
0.0.1	08/06/2016	Initial version due to PKI renewal
0.0.2	20/06/2016	Document review and errors correction
1.0.0	20/06/2016	Document Approval
1.0.1	19/09/2016	Modification LFE/2016/0071
1.0.2	23/11/2016	Modification (2) LFE/2016/0071
1.0.3	23/12/2016	Modification (3) LFE/2016/0071
1.0.4	29/05/2017	Adaptation to eIDAS Regulation

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

DOCUMENT CONTROL			
DRAFTED	**INSPECTED**	**APPROVED**	**ADMITTED**
PwC	Oscar 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 the General Directorate of Registers and Notary of the Ministry of Justice, are hereby established as a Certification Services Provider of 26 Of Law 24/2001, of December 27, on Fiscal, Administrative and Social Order Measures. It was born with the purpose of offering the necessary mechanisms and systems to guarantee the security of the telematics communications in which the Registrars, the Public Administrations, the professionals that deal with the Registers and the citizens in general take part.

The CORPME's TSP internal regulation is the basic certification standard service, which establishes its nature, structure and organization, as well as the criteria and procedures that the Service undertakes to comply with in the exercise of its activity. Starting from the request of the certificates and generation of keys to the subsequent issuance, distribution, use, revocation and renewal of the same.

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's Trust Service Provider will develop its activity in relation to digital certificate life Cycle application, issuance and management processes including certificates validity period verification, revocation and renewal 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 this CPS. In case of conflict or contradiction between the provisions of the Certification Practice Statement 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 Qualified 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 CPS assumes that the reader knows the concepts of PKI, certificate and Electronic Signature; otherwise, it is recommended that the reader is trained in the knowledge of the above concepts before continuing with the reading of this document.

1.2 Issue of SET test Certificates

CORPME's Trusted Services Provider issues a set of test certificates for both the regulatory body in the process of inspection or registration of new certificates and the developers of applications in the process of integration or evaluation for their acceptance, Have at their disposal certificates of the real hierarchy with fictitious data.

The data residing in these certificates are then provided so that third parties who rely on the CORPME Certification Hierarchy can verify that these certificates are without liability:

Entity name	[TESTS] ENTITY
NIF (Organization Identifier)	B00000000
Postal address	PLACE OF RESIDENT, 28001
Name	NAME
Surname	SURNAME1
Second surname	SURNAME2
DNI	00000000T
CVE (BOE)	000000000
Representation of Entity with Legal Personality	B00000000
DNS	test.corpme.es
Mail	pruebas@corpme.es
Collegiate society	COLLEGIATE SOCIETY
Local Management	LOCAL MANAGEMENT
Administrative Position	POSITION
Profession	PROFESSION

Not all the data shown here is reflected in all the certificates issued under the profiles that cover both this CPS and the associated CPs, but are used depending on its applicability to the corresponding certification profile.

In cases such as those indicated, the same versions of certificates are available in both physical format (keys generated in secure cryptographic devices) and in PKCS # 12 format (key storage software format). The SSI of the Provider of Trusted Services of CORPME guards the proof of possession's proof of the private key in both cases.

It is important to note that the tests for developers will preferably be performed with the CORPME TSP hierarchy of tests and will only be supplied if justified to avoid the propagation of this set of tests. They will also be revoked as soon as it determines CORPME's own TSP.

1.3 CPS Generalities

This CPS is issued taking into account the recommendations of the IETF (Request for comments) RFC3647: Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

CORPME will not issue Certificates of Legal Entity in so long as it is legally mandated that Certification Services Providers issuing Qualified Certificates not be obliged to issue such certificates, except in those profiles where they are explicitly determined in the This document and in the CP's themselves.

The issuance of digital certificates to other entities or corporations wishing to act as subordinate or secondary Certification Authorities, issuing digital certificates under the CORPME Root Certificate hierarchy, will require the express agreement of the Steering Committee, CORPME's highest governing body.

1.4 Document Name and Identification of the CPS

This document is called *CERTIFICATION PRACTICE STATEMENT.*

Document Identity:

Document Name	CERTIFICATION PRACTICE STATEMENT
Document version	1.0.4
Document status	Version
Broadcast Date	29/05/2017
Expiration Date	Not applicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.0.0.1.0.4
CPS situation	http://pki.registradores.org/normativa/index.htm

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

1.5.1 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 digital certificates.

The legal information and identifying data of the CORPME Certification Services 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:

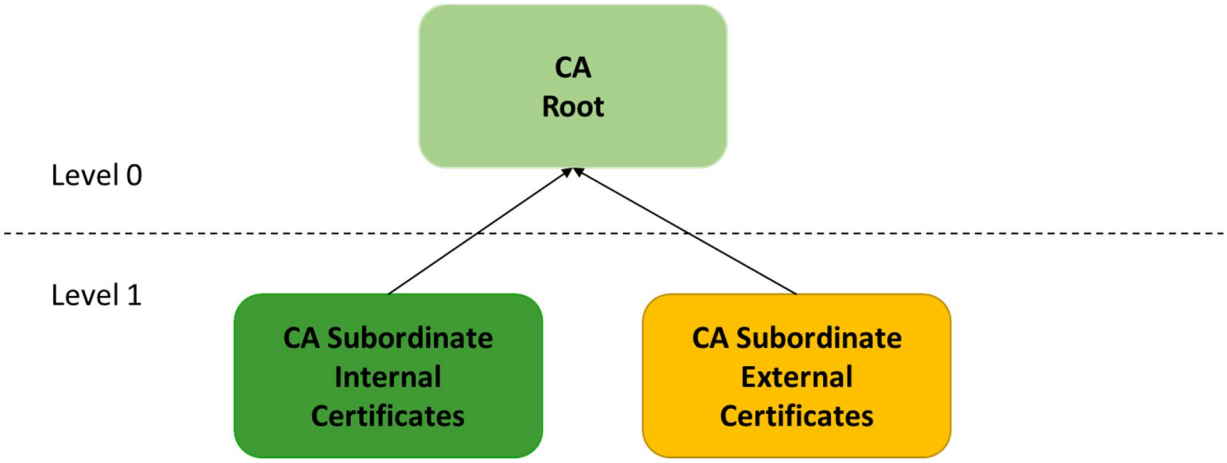
Colegio de Registradores de la Propiedad, Mercantiles y Bienes Muebles de España

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 Law 59/2003 of 20 December on Electronic Signature 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:



1.5.2 Policy approval authority

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

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

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.

1.5.3 Root Certification Authority

The CORPME issues all the certificates object of the present 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

1.5.4 Subordinated Certification Authorities

Under the hierarchy of CORPME´s main key or root certificate, are the certificates of the secondary key for internal certificates, as well as the secondary key for external certificates under whose respective hierarchies are issued all the certificates that CORPME emits to its final entities.

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

Distinctive name	CN = Autoridad de Certificación de los Registradores - CA 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 - CA 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.

1.5.5 Registration Authority

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

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

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

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

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

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

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

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

1.5.6 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).

1.5.7 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.

1.5.8 End entities

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

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

- Applicant.

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

1.5.8.1 Applicant

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

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

1.5.8.2 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 Certification Services Provider. Subscriber identification data is contained in the "Subject" field of the certificate defined within the ITU X509 standard.

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

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

The Subscriber identity as the holder of the certificate will appear in the Distinguished Name field of the digital certificate in the CN (*Common Name*), SN (*Serial Number*), 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.

1.5.8.3 Third parties that trust CORPME

For the purposes of this CPS, Third Party is any user who relies on the certificates issued by 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.

1.6 Classes of Digital Certificates and limits for their use

The digital certificates issued by CORPME are of several types:

- **PKI Own certificate**
  - Root CA Certificate.
  - The External Subordinate CA Certificate.
  - The Internal Sub CA Certificate.
  - The VA Certificate.
  - The TSA Certificate.
- Registry Operator Certificates.
- **Personal Certificates:**
  - Internal Certificates:
    - Registrar Qualified Certificate.
    - Internal Personnel Qualified Certificate.
    - Qualified Certificate of Legal Entity Representative for Electronic Invoicing.
  - External Certificates:
    - Personal Qualified Certificate.
    - Legal Person Representative Qualified Certificate.
    - Entity without Legal Personality Representative Qualified Certificate.
    - Administrative Position Qualified Certificate.
    - Qualified Certificate of Local Administration.
    - Local Administration Qualified Certificate.
- **Device Certificates:**
  - Non-Qualified Certificate for Registration Procedures.
- **Component Certificates:**
  - Generic SSL Non-Qualified Certificate.

1.6.1 PKI Certificates

PKI Certificates are those that support the private keys used by the Service for the signing of certificates and are the following: the root certificate and the hierarchy. The Certificate of the primary key or root is the *self-signed* certificate in which the trust chain is started. Directly subordinate, are the hierarchy certificates, which will be one for the internal certificates and another for the external certificates.

These certificates will have a key length equal to or greater than 2048 bits (being equal to 4096 bits for the Certificates of the Root and Subordinate Certification Authorities) and a validity of twelve (12) years, except for the Root CA, Which shall be twenty-four (24) years. The holder of the keys to the service is CORPME itself and are issued and revoked by the Central Processing Unit, at the request of the Steering Committee.

1.6.1.1 VA Certificate

That certificate used by the Validation Authority to sign the answers regarding the verification of the status of the certificates issued by CORPME TSP.

1.6.1.2 TSA Certificate

TSA is a certificate used by the TSA to sign the time stamp.

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 stamp 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 (TSU's) which will create and sign 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.

1.6.2 Registration Operator Certificates

The Registry Operator Certificates are certificates of personal use used by operators assigned to Processing Units for use in the exercise of the certification activity. All these certificates will be issued within the qualification profiles of Internal Personnel Qualified Certificate and / or Registrar Qualified Certificate. Each action taken on certificates is authorized by an order that must be signed with a key backed by an operator certificate.

There are two categories of certificates in this class:

- Operator of the Central Processing Unit.
- Registry Operator.

The Registry Operator Certificates contain the owner's name and email address, the name of the Destination Unit and its mailing address. The certified keys length will be at least 2048 bits and the validity of the certificates of two (2) years. Its owner is the operator and are issued and revoked by the Central Processing Unit, at the request of the Steering Committee in the case of the operators of this same Unit and at the request of the Registrars, in the case of the operators of the Processing Units of the Records.

1.6.3 Certificates for Service Communication

Those are intended for use by the automated processes that are used in the communications of the Service with the Processing Units or with the users. The certified keys length will be of 2048 bits and the validity of the certificates of two (2) years. The owner is the TSP of CORPME itself and are issued and revoked by the Central Processing Unit, at the request of the Steering Committee.

1.6.4 Personal Certificates

1.6.4.1 Internal Certificates

The internal certificates are professional and are made available to the holder only for use in activities related to their role within the registration organization.

1.6.4.1.1 Registrar Qualified Certificate

The Registrar Qualified Certificates are certified for personal use, and confirm the identity of the holder, as well as their status as employees of the Registrar. In addition, as might be the case: tax assessors in exercise and the Registrar, registration point or, if applicable, the Liquidation Office where they work. It will also include an indication of the special administrative destination in which the Registrar is located. The Registrar Qualified Certificates are issued for exclusive use in the scope of these functions.

The signatures backed by these certificates certify the personal intervention of the Registrar in all acts that are proper to his or her function, including all relations with third parties and are provided in the laws; as well as the elaboration of any type of document or certifications in electronic format. They are issued for exclusive use in the scope of these functions and relations with the Public Administrations.

The Registrar Qualified Certificates are used in the internal communications of the Registers, as well as to authorize the applications that the Registrar must send to the Central Processing Unit. They may also be used to ensure the authentication of its owner to systems that require it in an access control.

Registrar Qualified Certificates contain the name of the Subscriber Registrar of the certificate and its tax identification number, as well as the subscriber's email address, the name of the Registry of destination and its postal address.

1.6.4.1.2 Internal Personnel Qualified Certificate

Internal Personnel Qualified Certificate are certificates for personal use that certify the identity of the holder, as well as their status as an employee of the Registry, College, Dean's Office, College Society or employees in special situations. These are certificates for internal use and used for the relationships with the Public Administrations.

Internal Personnel Qualified Certificate contain the name of the employee subscribing the certificate and its e-mail address, as well as the name of the Registry or Unit of destination and its postal address.

1.6.4.1.3 Qualified Certificate of Legal Entity Representative for Electronic Invoicing

The Qualified Certificate of Legal Entity Representative of the for Electronic Invoicing proves the identity of its holder, who will always be a natural person, and its status as representative of a legal entity that will always be the Registrar's Association, and its status as a member of the Governing Board. They can only be used to sign the documents related to electronic invoicing and their use is limited to the signing of invoices.

In addition to the identification of the Subscriber and the Registrar's Association as a legal entity, it shall contain information on the Subscriber's relationship with the Company, reflecting his / her position within the Board of Governors.

The Central Processing Unit of CORPME will issue these certificates under an approved application according to the application management procedure and validated by the CORPME's Technical Director of SSI.

1.6.4.2 External Certificates

Unless otherwise stated in the CP's, certificates issued under the secondary code for external certificates may be used only in registrable acts and in the communications that are made between its holder and the Registers, Public Administrations and other types of Organizations and Entities, in accordance with the provisions of their respective CP.

The subscriber must refrain from using them for any purpose other than authorized and, if this obligation is not fulfilled, in any case the signatures backed by these certificates will have effects vis-à-vis third parties. This circumstance shall be expressly stated in the content of the certificates themselves.

The external certificates will be authorized and revoked by the Processing Units, according to the procedure established for each of their classes.

1.6.4.2.1 Personal Qualified Certificate

Personal Qualified Certificates certify the owner's identity, who will always be a natural person. They may only be used to sign the documents submitted to the Registers, Public Administrations and other types of Entities and Entities, as well as in the communications made with them, guaranteeing the authenticity of the issuer, non-repudiation of origin and Integrity of content. They can also be used to ensure the owner's authentication to systems that require access control and signature of emails.

Personal Qualified Certificates have as main purpose the signing of documents, guaranteeing the authenticity of the issuer of the communication, the non-repudiation of origin and the integrity of the content. Personal Certificates can also be used to ensure the holder's authentication to systems that require access control. Personal Qualified Certificates will identify their holder in the different fields of the DN field attribute (*Distinguished name*) that contains the name, surname and tax identification number (NIF, NIE, passport or other), without the admission of Use of pseudonyms.

In the absence of a NIF, the national identity card number or, in the case of foreigners, the alien identification number, the passport number, the residence card number or any other legal identification document may be included.

The address, telephone and fax numbers and subscriber's email address may also be included in the certificate, as provided in the corresponding CP.

1.6.4.2.2 Legal Person Representative Qualified Certificate

Legal Person Representative Qualified Certificates represent the identity of the holder, who will always be a natural person, and his status as organic representative or volunteer of a legal entity. They are issued for use, mainly and in accordance with the particular CP's, for the signing of documents, guaranteeing the authenticity of the issuer, non-repudiation of origin and the integrity of the content. Legal Person Representative Qualified Certificates may also be used to ensure the holder's authentication to systems that require access control and signature of emails.

The Legal Person Representative Qualified Certificate, in addition to the identification of the Subscriber and the Company, shall contain information on the representation relationship that the subscriber holds with respect to the Represented Company. These certificates will contain the Registration data that are recorded at the time of issuance in the Business Registry.

In case of disagreement between the data of representation incorporated in the certificate and the workers in the Business Registry, the latter will always prevail.

1.6.4.2.3 Entity without Legal Personality Representative Qualified Certificate

Entity without Legal Personality Representative Qualified Certificates accredit the identity of its holder, who will always be a natural person, and its status as holder or organic or voluntary representative of an Entity without registered legal personality. They are issued for use, mainly and in accordance with the particular CP's, for the signing of documents, guaranteeing the authenticity of the issuer, non-repudiation of origin and the integrity of the content. Entity without Legal Personality Representative Qualified Certificates may also be used to ensure the holder's authentication to systems that require it in an access control and signing of emails.

The Entity without Legal Personality Representative Qualified Certificate, in addition to the identification of the Subscriber and the Company, shall contain information on the representation relationship that the subscriber has with respect to the Represented Company, including a unique electronic identifier of the Official State Gazette describing such representation, and which links the certificate with the Electronic Validation Code (CVE) of the submitted document.

1.6.4.2.4 Administrative Position Qualified Certificate

Administrative Position Qualified Certificates certify the identity of the holder, as well as his status as an official belonging to the State or autonomous Administration. They are issued for their exclusive use in the scope of their official activity and their relationship with the Registers through the interactive services provided by CORPME. They are issued for the signature of documents, guaranteeing the authenticity of the issuer, the non-repudiation of origin and the integrity of the content. Administrative Position Qualified Certificates may be used to ensure the holder's authentication to systems that require access control and signature of emails.

The signatures backed by these certificates accredit the personal intervention of the official in all the acts that are proper to his position, including the communications and the elaboration of all type of documents in electronic format.

The Administrative Position Qualified Certificates have as main purpose the signing of documents, guaranteeing the authenticity of the issuer, the non-repudiation of origin and the integrity of the content. Administrative Position Qualified Certificates may also be used to ensure the holder's authentication to systems that require it in an access control.

1.6.4.2.5 Local Administration Qualified Certificate

Local Administration Qualified Certificates accredit the identity of the holder, as well as their status as an official or position belonging to the Local Administration. They are issued for their exclusive use in the scope of their official activity and their relationship with the Registers. They are issued for the signature of documents, guaranteeing the authenticity of the issuer, the non-repudiation of origin and the integrity of the content. Local Administration Qualified Certificates can be used to assure the authentication of its holder to systems that require it in an access control and the signature of emails.

The signatures backed by these certificates accredit the personal intervention of the official in all the acts that are proper to his position, including the communications and the elaboration of all type of documents in electronic format.

The Local Administration Qualified Certificates have as main purpose the signing of documents, guaranteeing the authenticity of the issuer, the non-repudiation of origin and the integrity of the content. Local Administration Qualified Certificates can also be used to ensure the authentication of its owner to systems that require it in an access control.

1.6.4.2.6 Professional Qualified Certificate

Professional Qualified Certificates certify the identity of the holder, and their membership in a profession regulated and subject to the discipline of a Professional Association or Association. Its main purpose is to sign documents submitted to Registers and Public Administrations, and their use in all communications made with them. They are issued for the signature of documents, guaranteeing the authenticity of the issuer, the non-repudiation of origin and the integrity of the content. Professional Qualified Certificates can be used to ensure the holder's authentication to systems that require it in an access control and the signing of emails.

Under a specific agreement between CORPME and the Professional Collectives, the scope of use of the CORPME digital certificates can be extended to allow their use in the acts of their turn or activity. Serving in such a case, in addition to its primary function, to guarantee the intervention of the professional in the business and telematics procedures in which it participates in that condition, including the communications and the elaboration of all type of documents in electronic format.

Professional Qualified Certificates guarantee the identity of the issuer, non-repudiation of origin and integrity of the content of documents and communications. They might also be used to ensure the authentication of its owner to systems that require it in an access control.

1.6.5 Component Certificates

1.6.5.1 Non-Qualified Certificate for Registration Procedures

Non-Qualified Certificates for Registration Procedures support signatures automatically made by the computers of the Registers destined for this purpose and, in addition, allow them to authenticate themselves to the users, as well as to establish session ciphers in the communications that they make. The holder will be, at any moment, the Registrar in charge of the Registry for which they have been issued.

The main function of these certificates is to allow the sending of electronic documents, proving the receipt by the Registry of a signature or electronic document and the time at which it occurred (time stamp).

1.6.5.2 Generic SSL Non-Qualified Certificate

Unsecured SSL server certificates link signature verification data to a computer application on a server with SSL support.

On these certificates, there will be a responsible person who will be a natural person who will have the control to act on the certificate.

CORPME Central Processing Unit will issue these certificates under an approved request according to application management procedure and validated this request by CORPME SSI Technical Director.

1.7 Generic Limitation on the use of certificate

The digital certificates issued by CORPME shall be used, solely and exclusively for the purpose for which they were issued, in accordance with the provisions of this CPS, the particular CP's and the Internal Regulations of the TSP. As indicated in the previous section, the generic limitation of use may be modified under the agreements that CORPME subscribes with a certain collective or association, in order to cover other uses other than the authorized primary.

Likewise, certificates should be used only in accordance with the applicable legislation, especially taking into account the existing import and export restrictions on cryptography.

The certification services offered by CORPME have not been designed or authorized to be used in activities of high risk or requiring a fail-safe activity, such as those related to the operation of hospital, nuclear, air traffic control or railway facilities, or any other activity where failures could lead to death, personal injury or serious damage to the environment.

Each CP will establish specific limitations on the use of its certificates.

1.8 Definitions and Acronyms

1.8.1 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 the Certification Practices Statement, 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. For the purposes of this CP, Certification Authority are all those that are defined in it.

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 Certification Practice Statement.

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 the Certification Practice Statement, 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.

1.8.2 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.

1.9 CPS Administration

1.9.1 Responsible entity

The Information Systems Service (hereinafter ISS) 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 Office of Security and Regulatory Compliance, who will act as Secretary.
- The Director of Infrastructures, Security Engineering and Communications.
- Wintel Technology Director and Virtualization.
- The Director of Operations.
- A Director of Projects and Services, representing the Directors of Projects and Services.

Establish the terms and wording of the CORPME CPS. In those cases where, in accordance with the provisions of the TSP Rules of Procedure, it is mandatory, the Steering Committee shall act by mandate of the Board of Governors of the College of Registrars, or obtain its authorization in those matters whose competence is reserved to the Government of the Registrars.

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.

1.9.2 Procedure for approval and modification of the Certification Practice Statement

The approval and subsequent modifications of the CPS shall be the exclusive responsibility of the Executive Committee, in accordance with the powers delegated by the CORPME Governing Board, in accordance with the provisions of the TSP Rules of Procedure.

Any modifications to this CPS 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 and voluntary revocation by the user that is not in accordance with the provisions incorporated because of this CPS, will not grant the subscriber any right to be compensated for this reason.

1.10 Contact details

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

Colegio de Registradores de la Propiedad, Mercantiles y 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

2 DIRECTORY AND PUBLICATION OF CERTIFICATES

2.1 Certificate validation directory

The CORPME maintains a Certificate Validation Directory that is 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 CP's 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 Initial registration

3.1.1 Name Types

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

3.1.2 Need for names to be meaningful

In all cases, it is recommended that the names of the subscribers of the certificates be significant.

In any case, the endowment of the distinctive names of meaning is given by the policy to that effect developed and described in the CP document corresponding to the certificate in question.

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 plus the contents of the "*Certificate Policies*" extension. Policy Identifier must be unique and unambiguous.

Each CP will establish the unique name uniqueness mechanism.

3.1.5 Conflict resolution procedure

As established in section 9.13 of this document.

3.1.6 Recognition, Recognition, authentication and trademarks role

Not stipulated.

3.2 Initial identity validation

3.2.1 Private Key Possession Proof

The key pair is generated by the secure cryptographic device of the applicant and under its custody, so that the possession of the private key corresponding to the public key for which the requestor requests the certificate to be generated will be proved by the Submission of the Certificate-Signing Request (CSR).

This procedure may be modified by establishing in each case the applicable CP.

3.2.2 Authentication of Identity for Legal Persons

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

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

Besides the applicant identification by checking the above mentioned documentation, the corresponding 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 national applicants for CORPME's Certificates must appear before the Processing Unit of their choice, with their NIF, NIE, passport or other identification document.

Foreign applicants for 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.

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

If the registration corresponding to the attributes is accessible through the Internet, the Operator of the corresponding Processing Unit must include in the certificate the code that allows direct access to its contents.

In the case of the other attributes, the Operator of the corresponding Processing Unit must carry out the documentary checks provided for in the corresponding CP's, keeping a copy of the documents indicated by them. It will also verify the equivalence between the literal terms and term of the documented attributes and their expression in the certificate.

Membership of Professional Associations, i.e. Colleges or Associations, will be credited for the purposes of the issuance of Professional Qualified Certificates, through the contribution of Certification signed by the Secretary of the Association or Association to which the Applicant is attached, issued a maximum Of fifteen (15) days before the appearance in the corresponding Processing Unit.

By virtue of an agreement, CORPME and the Professional Collective interested in obtaining Professional Qualified Certificates for its members may establish procedures for validation of alternative attributes to the certification contribution of the collective secretary, namely technical procedures for interconnection between CORPME and Repositories of the professional group, for online verification of the applicant's membership of said group.

The technical and procedural measures necessary for the protection of the Personal Data of the Collegiate or Associated persons included in the automated verification file shall be adopted in the interconnection and access to the applicant's membership data.

3.2.4 Information not verified about the Applicant

All the information presented by the applicant is verified before the issuance of the certificate that requests.

3.2.5 Representation Powers Verification

The corresponding CP will describe the procedure for verifying the applicant's powers of representation.

3.2.6 Criteria for operating with external CA's

In order to establish interactivity relationships with external CA's, the CORPME TSP will establish certain security requirements to ensure the adequacy of these external CA's to the CORPME PKI.

The following security requirements defined may be extended in each case by the PAA, as it deems appropriate:

- The external CA must provide a level of security in the management of the certificates, throughout its life cycle, at least, equal to the CORPME TSP. The CA will collect in the corresponding CPs and CP's and in their compliance this requirement.
- You must provide the audit report of an external authority of recognized prestige regarding your operations as a means of verifying the existing level of security. The PAA may declare exempted from this requirement to the CA's it deems appropriate.
- Establish a collaboration agreement setting out the security commitments made for the certificates included in the interaction. Likewise, the PAA may deny the request for interactivity without the need to provide any justification, even if the external CA meets the requirements defined above.

Interactivity can be accomplished through cross-certification, unilateral certification or other forms.

3.3 Identification and authentication for renewal requests

The identification and authentication of the holders of the certificates for the renewal requests for any reason, which are specified in section 4.7 of this document, will be made through the process of issuing certificates, i.e., NIF, NIE, Passport or other identification document of the holder.

In addition, the Operator of the corresponding Processing Unit will request the documentation proving the certifiable attribute in question under the Type of Certificate, except for Legal Person Representative Qualified Certificates, where the Operator will confirm by its means the supporting documentation of the applicant.

Likewise, the Processing Units will be responsible for the filing of all documentation related to the certificates and their applications, and must be filed for a minimum of fifteen (15) years.

3.4 Identification and authentication for revocation requests

The identification and authentication of the holders of the certificates for the revocation requests for any reason, which are specified in section 4.9 of this document, will be made through the NIF, NIE, passport or other identification document of the holder.

For Non-Qualified Internal Certificates (for Registration Procedures and SSL), the Central Processing Unit will identify the holder through the corporate email used in the certificate request.

4 OPERATIONAL REQUIREMENTS FOR CERTIFICATES LIFE CYCLE

The process of issuing digital certificates process begins with the appointment request and the user's registration in the CORPME agenda: **https://www.registradores.org/scr/agenda.**

The generation of the key pair will be performed within a secure cryptographic device and with the personal intervention and custody of the certificate applicant, who will also introduce passwords for accessing the private key by himself.

4.1 Application for certificates

4.1.1 Who can make an application

Each CP specifies who can request a certificate and the information that must be provided in the application. In addition, the CP establishes the steps that must be followed to carry out this process.

In general, in relation to the application procedure for certificates, two cases are distinguished:

1. **Need to request an appointment**

   In cases where a prior appointment is requested (Personal Qualified Certificate, of Legal Person Representative Qualified Certificate and Professional Qualified Certificate) as a preliminary step to obtain the certificate, the applicant Connects to the website **https://www.registradores.org/scr/agenda**. In case you are not registered in the system, you must register as a user. Once registered, you must complete an online form, 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 of Use of the certificate will be generated. Certificate.

   Since License for Certificate Use must be signed by the Registry Operator 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 enabled by the Operator of the same, as skilled for the issuance of digital certificates. Once the date and time have been set for the appearance, the applicant will receive by e-mail a proof of the arranged appointment.

2. **No need to request a prior appointment**

   In the cases that do not require an appointment (Registrar Qualified Certificate, Internal Personnel Qualified Certificate, Qualified Certificate of Legal Entity Representative for Electronic Invoicing, Administrative Position Qualified Certificate, Local Administration Qualified Certificate and Entity without Legal Personality Representative Qualified Certificate), a false appointment will be created to request And validate the user's data and proceed to invoke the issuance of the certificate. Users requesting Qualified Certificates will be presented with a corresponding identification document and a certificate accrediting the charge, and for applications for Non-Qualified Certificates, the request will be sent by e-mail and will be issued by the Central Processing Unit of CORPME.

4.1.2 Registration of request and applicants' responsibilities

In both cases, the applicant is a person in the processing unit with the identifier of the appointment, with the NIF, NIE, passport or other identification document and the certification that accredits the charge for the case of request for Administrative Position Qualified Certificate and Local Administration Qualified Certificate. This identifier will be delivered to the Registry Officer who enters it into the system (retrieves the data previously entered). Again, the authentication checks described in section 3.2.3 of this document are repeated and, if they are correct, the next point will be taken.

With the appearance of the user, in a single instance, the process of verification of identity and certifiable attributes, to the process of issuance of the Digital Subscriber Certificate, which is signed by the CA in order to establish the chain of trust on which the Qualified Electronic Signature is based.

Once the identification process and, where appropriate, the verification of attributes of the applicant, the license of use will be transmitted in electronic format to the applicant and the Operator will print two copies of the license of use, which will contain the date, Data's certificate, the Registry Operator and the name of the same. The applicant and the operator, a copy being kept by each of them, must sign both copies.

The unit where processing was carried out must keep the signed license for a period of fifteen (15) years, counting from the expiration or revocation of the certificate.

Once the identity of the applicant and the necessary data have been validated, the requested certificate is issued.

4.2 License Applications Processing

4.2.1 Performing identification and authentication function

For the natural person authentication, for both nationals and foreigners, and of the documentation proving the certifiable attribute in question by virtue of the type of certificate, the procedure set out in section 3.2.3 of this document will be followed.

4.2.2 License application approval or rejection

The issuance of the certificate will take place once the CORPME TSP has carried out the necessary verifications to validate the certification request.

CORPME's TSP may refuse to issue a certificate from any applicant based exclusively on its own criteria, without incurring any responsibility for the consequences that may arise from such refusal.

4.2.3 Deadline for license applications processing

CA's of the TSP of CORPME are not responsible for delays that may arise in the period between the request of the certificate and the delivery of the same. In any case, when the appointment is required for the certificate issue, no delays are expected in the processing of the certificate requests, except for those caused by technical incidents outside the normal operation of the CORPME TSP.

4.3 Certificates Issuance

4.3.1 CA actions during certificate issuance

Once the previous procedures have been completed, the keys will be generated and, if necessary, the issuance of the requested certificate.

For the issuance of the Qualified Certificates and the generation of the key pair, secure cryptographic devices will be used, in which the key pair generation and the signature cryptographic operations will be performed directly and immediately, in such a way that all The functionalities provided in the CP's are carried out without, in any case, it is necessary to transfer the private key (signature creation data) to an external equipment, thus guaranteeing the subscriber in this way his absolute control over the signature creation data, And therefore, the impossibility of supplanting its Electronic Signature. The holder of the certificate will carry out the order of generation of the keys and the introduction of the passwords of the cryptographic device personally.

Both QSCD's and file formats used in the certificate issuance process conform to RSA Data Security Inc.'s Public-Key Cryptography Standards (PKCS) standards.

In the case of QSCDs, these will be in accordance with the technical standards (CWA: CEN WORKSHOP AGREEMENTS) issued by the European Committee for Standardization (CEN) in accordance with Directive 1999/93 establishing a Community framework For the Electronic Signature. Safety approvals are detailed as follows:

- Common Criteria EAL4+, FIPS 140-2 y CC EAL4+ PP-SSCD.
- Compatible with specifications ISO 7816-1 a 4.

4.3.2 Notification to the applicant of the issuance by CA of the certificate

The certificate request include the interested email, so an email is sent notifying the applicant the certificate issue by the CA. This email will include a code, which allows the holder to carry a cable revocation of the certificate remotely through a phone call.

When any of the CA's issues a certificate according to a request for certification processed through an AR, it will facilitate the consultation of the certificates issued for those authorities concerned.

4.4 Certificate acceptance

4.4.1 Certificate Acceptance mechanism

The acceptance of the certificate is the action by which its subscriber initiates its obligations with respect to the CORPME TSP.

The certificate subscriber must accept it by signing the license. In no case will a person holding a certificate be considered before signing the corresponding license and the license is in the possession of the corresponding Processing Unit.

The content of the license use is specified in the corresponding CP. In the license of use, the signatory must expressly commit to fulfil the obligations listed throughout the document and accept:

- That each digital signature created using the private key corresponding to the certified public key is the Subscriber's Electronic Signature.
- That each time the subscriber uses their certificate to access any type of information, he has made such access personally.

- The use of the certified private key is personal and non-transferable, so any use made of it by third parties will be under the responsibility and risk of the subscriber. The subscriber will declare to have exclusive control over the Signature Creation Data (private key) associated to the Signature Verification Data (public key) included in the certificate issued in his name by CORPME.
- That you accept the limitations of use corresponding to the type of certificate in question and, in any case, that you will not use the private key corresponding to the public key certified for the purpose of signing certificates or lists of revoked certificates.
- That you agree to the terms and conditions contained in this document and in the corresponding CP's.
- All data provided during user registration and certificate request are entirely accurate.
- That the certificate will be used in strict accordance with the legality and with the conditions established in the CPS and in the particular CP's that are applicable by virtue of the type of Certificate in question.

4.4.2 Publication of certificate

The CORPME TSP will not publish personal certificates issued in any web directory, since all Qualified Certificates are generated directly within a QSCD, and in no case are issued in software support. The certificates of devices will be generated in both devices and software and will not be published in any web directory.

4.4.3 Certificate issuance notification by CA to other authorities

When one of the PKI CA's of the PKI of CORPME issues a certificate according to a request for certification processed through an AR, it will facilitate the consultation of the certificates issued for those authorities concerned.

4.5 Key pair and certificate usage

4.5.1 Use of the private key and certificate by the holder

In any case, the holder may only use the private key and the certificate for authorized uses in the corresponding CP and in accordance with the *'Key Usage'* and *'Extended Key Usage'* certificate's fields.

In the same way, the holder can only use the key pair and the certificate after accepting the use's conditions, established in the CPS and CP, and only for what they establish.

Upon expiration or revocation of the certificate, the holder will no longer use the private key.

4.5.2 Use of public Key and certificate by third party acceptors

Third parties who trust can only place their trust in the certificates in accordance with the *'Key Usage*' and *'Extended Key Usage'* certificate's fields.

The trusted third parties must perform the public key operations in an appropriate manner to trust the certificate, as well as assume responsibility for verifying the status of the certificate using the mechanisms established in this CPS and in the corresponding CP.

Likewise, they adhere to the conditions of use established in said documents.

4.6 Certificate Renewals without Key Change

4.6.1 Circumstances for renewing certificates without a change of Keys without a change of key

The certificates renewals made in the scope of this CPS will always be carried out with a change of keys.

4.6.2 Who can request the renewal of certificates without change of keys

Not stipulated.

4.6.3 Certificate Renewal Request without key Change Processing

Not stipulated.

4.6.4 Notification of renewal 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

The digital certificates issued by CORPME are subject to renewal as long as they are with a change of keys. Expiry or extinction of a digital certificate, due to the expiry of the validity period, it is only possible to request a new digital certificate.

4.7.1 Circumstances for the renewal of certificates with change of keys

The following are the causes for a CORPME certificate renewal:

- Expiration of the certificate period of validity.

  The certificate has undergone changes of format.

4.7.2 Who can request renewal of certificates with change of keys

The following are entitled to request a revocation of a certificate:

- The holder of the certificate or subscriber.
- The legal representative, duly authorized.
- When applicable, the person other than the subscriber who has previously requested the certificate and holds a charge that authorizes him to make such request.

4.7.3 Processing of certificate renewal requests with keys change

The request for renewal of the certificate can be treated in the following ways:

- **Face-to-face:** It is carried out in the same way as a revocation and procurement of certificates in person, but carried out jointly. Details of these processes can be found in the Procurement and Revocation procedures.
- **Remote:** Applicable to users with an active certificate, within the renewal period defined as two (2) months prior to the expiration date. The remote renewal will be allowed just once, and the next one the user is obliged to renew in person, as dictated by the rules of Electronic Signature. The certificate holder will receive two (2) months before the expiration date of the certificate, a notification containing a link to carry out the renewal process remotely. This link will redirect to a website requesting the electronic certificate to be renewed and, later, verifying the certificate meets the renewal assumptions. If the renewal is authorized, a revocation and procurement of certificate will be carried out, sending the related notifications to the holder. The renewal process is immediate. In the case of remote renewal, the owner will implicitly accept the license of use signed in the initial certificate issuance.

4.7.4 Notification of the renewal of a certificate to the holder

The notifications to the certificate holder associated with the renewal process will be the same than in the process for certificate revocation and procurement. Therefore, the revocation of the current certificate will be notified first and then the issuance of the new certificate.

The holder will have the obligation to check if the revocation has been published in the CRL.

4.7.5 Acceptance of certificate with change of key

The holder as established in section 4.5.1 of this document will make acceptance of the certificate.

4.7.6 Publication of the certificate with key change by the CA

Not stipulated.

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

Not stipulated.

4.8 Certificates modification

The digital certificates issued by CORPME are not subject to change. When the modification of any data contained in the certificates is required, it will be renewal with the corrected data.

On the one hand, certificates modifications derived from the following reason:

- Name change.
- Change in functions within the organization.
- Reorganization because of the change in the distinctive name.

On the other hand, certificate modifications derived from the following causes will be treated like remote renovations:

- Key length Change.
- Signature algorithm change.

4.8.1 Circumstances for the modification of a certificate

Not stipulated.

4.8.2 Who can request certificates modification

Not stipulated.

4.8.3 Processing of certification modification request

Not stipulated.

4.8.4 Notification of the modification of a certificate to the holder

Not stipulated.

4.8.5 Acceptance of the modified certificate

Not stipulated.

4.8.6 Publication of the 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

The revocation certificates implies the loss of its effectiveness, its consequences being equivalent to those of expiration. The revocation certificate will produce effects against immediate third parties through OCSP and from the moment, the CRL list containing the revocation is published.

4.9.1 Circumstances for revocation

The following are the causes for the revocation of a CORPME digital certificate:

- if requested by the subscriber of the certificate, or the person legitimized for the request of the same, or the one represented in the Certificates of Representative, request it.
- if the subscriber of the certificate ceases at its destination in the case of internal certificates.
- If a new certificate is issued for the same subscriber that refers to identical attributes, in the case of external certificates.
- To cancel or modify an inscription that refers to the content of an attribute certificate based on a registration.
- The support in which the private key corresponding to the public certificate is contained results lost or disabled.
- That a third party had misused the private key corresponding to the certified public.
- That the private key corresponding to the certified public has been unveiled or could have been compromised by any circumstance.
- That the subscriber has died or has been legally incapacitated or, if applicable, has lost, definitively or for a period exceeding the term of validity of the certificate, the condition or position by virtue of which the certificate was issued, Any cause, extinguishes the legal entity to whom the position or proxy holder of the certificate represents.
- That the information contained in the certificate or the data provided by the owner during the registration process, are inaccurate, whether due to initial error or falsity of the subscriber or due to changes.
- That the certificate has undergone format changes.
- That the subscriber has not complied with the provisions of this CPS or any of the CP's.
- That this be done in an administrative decision, in a decision, or in the case of internal certificates, in a disciplinary file.

4.9.2 Who can request revocation

The following entities are entitled to request revocation of the certificate:

- The certificate´s holder or subscriber.
- The legal representative of the subscriber, duly authorized.
- The entity represented by the subscriber of the Representative Qualified Certificate, through its governing body.
- When applicable, the person other than the subscriber who has previously requested the certificate and holds a charge that authorizes him to make such request.
- In the certificate of attributes based on a registration, the Registrar authorizing the modification or cancellation thereof.
- The Dean of CORPME, or the one in which he delegates, the Technical Director of the SSI, or the Registrar responsible for the Processing Unit who authorized the issuance of the certificate, when they have evidence of the existence of any of the causes mentioned in item previous.
- The judicial or administrative authority by virtue of a reasoned decision.

4.9.3 Revocation request procedure

4.9.3.1 Revocation at the request of the certificate subscriber

Revocation can be done in two ways:

- **Face-to-face:** The holder may revoke the certificate by appearing in the Processing Unit that issued the certificate or, in case of emergency, in any other CORPME Processing Unit. Once the holder has been identified, the Registry Officer will print a revocation request and, once it is signed by both, will immediately order the revocation of the certificate. In any case, the owner must complete the application form with his personal data, indicating the cause of the revocation request.
- **Remote:** The holder may revoke the certificate remotely by means of a telephone call, or by signing an electronic application. For the first method, it is need to call to the Telephone Assistance Service and the revocation will take effect in that very moment, after the necessary checks to guarantee the identity of the applicant. Throughout the process, the communication will be recorded and registered serving as support and guarantee of acceptance of the revocation request. This service is provided through the telephone number +34 912701771.

  First, the identity of the user making the call will be verified, checking the personal information regarding the type of certificate and attributes of the subscriber.

  Subsequently, the identity will be credited by the revocation code provided to the user during the issuance of the certificate.

  In the event of forgetting or losing the revocation code, this code will be re-sent to the e-mail provided in the certificate issuance process and, in this way, the revocation process can be continued.

  In case the identity of the user making the call does not correspond to the information of the signatory of the certificate, it will be indicated that it is not possible to carry out the revocation by telephone, and it will have to be contacted with CORPME to proceed with the Revocation by another stipulated method.

  For the electronic application signature method, the revocation will also take effect in that very moment. In this case, the user identification will be carried out with a valid certificate of the user's own. To carry out this type of revocation, the applicant will have to access the link: http://pki.registradores.org/, download the electronic application, sign it and send it to the email: revocaciones@corpme.es. Afterwards, you must contact the Telephone Assistance Service to confirm the receipt and obtain from the PSC the confirmation that the process has been carried out correctly.

4.9.3.2 Revocation by person other than titular subscriber

The person who holds the position that legitimates the request for a particular type of certificate, or that represented in the Representative Qualified Certificates, may order the revocation.

To do this, a signed request must be send to the Processing Unit where the certificate was issued. Once it verifies the capacity of the person to act on behalf of the owner, the Processing Unit will proceed to the revocation of the certificate, under the sole responsibility of the applicant for the revocation.

4.9.3.3 Revocation of profession

Certificates may be revoked by the Central Processing Unit or by the Registrar in charge of any of the Processing Units when any of the causes indicated in this document are present.

The administrative decisions and judicial decisions must be executed in the internal certificates by the Governance Board who will send the corresponding order to the Central Processing Unit and, in the external certificates, by the Registrar responsible for the Processing Unit where the certificate was issued.

Upon receipt of the revocation order, the Processing Unit, central or provincial, as appropriate, must immediately revoke the certificate indicating to the certificate holder the fact and cause of the revocation.

The Processing Unit shall keep a copy of the administrative decision or document on which the revocation order is based.

4.9.3.4 Revocation because of urgency

The Central Processing Unit may authorize the revocation of a certificate as a matter of urgency, when it is required by any of the persons mentioned in this document.

Once verified the identity of the revocation applicant, The Central Processing Unit can request a justification until satisfying the requirements demanded by the CPs for the cause of revocation alleged. If such justification is not possible or if the revocation has caused damages to third parties, the responsibility will only be on the applicant for the revocation.

This revocation will take effect in that very moment, after the necessary checks to guarantee the identity of the applicant. The revocation of a certificate assumes its total loss of validity and the exemption of responsibility of the Certification Service for any damage caused as a result of the use of the certificate revoked after its revocation.

4.9.4 Grace Period of the Revocation Request

There is no grace period for a validated revocation request. The revocation will have effects against the applicant from the moment he submits the corresponding request to the Processing Unit and, against third parties, since it is published in the Directory of Revocation Lists.

4.9.5 Term on which the CA must resolve the revocation request

Generally, requests for revocation will take effect at the time they are requested, always after the checks necessary to guarantee the identity of the applicant.

In case of an exceptional incident preventing the immediate revocation, a maximum time of 24 hours is established for the processing of revocations.

4.9.6 Verification requirements for revocation by trusted third parties

In good faith, third parties must verify, before depositing their trust in a CORPME certificate, the validity and validity of the certificates using the OCSP service or by accessing the last list of Revoked Certificates (CRLs).

4.9.7 CRL Emission Frequency

Revoked certificates are included in a revoked certificate list (CRL), which is updated as soon as a new revocation occurs, with the new list being published in less than one (1) minute from the revocation produced, at the URLs identified in Section 2.1 of this document.

The published CRL indicates the date and time information of the next scheduled broadcast.

4.9.8 Maximum time between CRL generation and publication

Regardless of the occurrence of new revocations, a new revocation list (CRL) digitally signed by CORPME shall be issued every twelve (12) hours in the case of the Subordinated CA's, and one (1) year of the CA Root, without prejudice of the reissue of a new list with each revocation practiced.

4.9.9 Availability of online system for verifying certificate status

The certificate status checking service will be kept accessible and available to users and third parties on a permanent basis, in order to facilitate verification of the validity of the certificates.

In order to ensure the availability of the Certificate Validation Directory server as well as the OCSP service, redundant and delocalized systems have been set up to minimize any disruption to the service.

4.9.10 Online Revocation Checking Requirements

Third parties, who rely on the Validation Authority to check online the revocation of a certificate, must have software that is capable of operating with the OCSP protocol.

4.9.11 Other forms of disclosure of revocation information available

CP's support the use of CRL's Distribution Points (CDPs) as another form of disclosure of available revocation information.

4.9.12 Special Requirements for Committed Key Revocation

There is no variation in the previous clauses when the revocation is due to the commitment of the private key.

4.9.13 Causes for suspension

CORPME only contemplates two possible states for the digital certificates it issues, which may be found valid or revoked.

In those cases in which the validity of the certificate is challenged by circumstances arising from the issuance, an ex officio revocation of the certificate will proceed, in accordance with the provisions of the corresponding section of this CPS.

The revocation of office made in the cases indicated, will not grant the Subscriber the right to other compensation different from the exemption of the costs associated with the issuance of a new digital certificate of the same class as the revoked.

In the issuance of the new certificate, the same formalities and procedures will be observed in all cases as with the original certificate revoked ex officio.

4.9.14 Who can request suspension

Not stipulated.

4.9.15 Procedure for requesting suspension

Not stipulated.

4.9.16 Limits of the suspension period

Not stipulated.

4.10 Certificate Status Information Services

4.10.1 Operating characteristics

The CORPME TSP has two (2) services that provide information on the status of the certificates issued by its CA:

- **Publication of certificate revocation lists (CRLs)**. Access to CRLs is done via HTTP, at the addresses published in section 2.1 of this document.
- **Online validation service (Validation Authority, VA)** that implements the Online Certificate Status Protocol (OCSP) following RFC6960. By using this protocol, it is possible to obtain the status of an electronic certificate without requiring the CRLs by directly consulting the VA.

4.10.2 Service Availability

The service, in its two variants (CRLs and OCSP), is available uninterrupted every day of the year, both for the trusted third party and for the holders of certificates or other parties that require them.

4.10.3 Additional features

CORPME will in no case provide an OCSP client to make use of the Online Validation Service. It is the responsibility of those who wish to use this service to have an OCSP client that complies with RFC6960.

4.11 Expiry of the validity of a certificate

In addition to the extinction of the certificate due to the exhaustion of the period of validity, CORPME certificates will be extinguished in the following cases:

- Death of the certificate holder.
- The incumbent, or legal guardian assigned, will be responsible for transmitting the loss of capacity or Disqualification of the subscriber, decreed judicially.
- In the case of Certificates of Representative of Legal Person: revocation of the organic or voluntary representation, since it access to the Business Registry; or loss of the legal personality of the Company represented, for any of the legal cases of dissolution or corporate extinction.
- Dissolution or termination of the CORPME Certification Services Provider activity.
- Firm resolution relapsed in judicial or administrative headquarters that orders the revocation of the certificate of the subscriber.
- Violation or endangered of the secrecy of the signature creation data of the signatory or the service provider of certification or misuse of said data by a third party.
- Alteration of the data provided to obtain the certificate or modification of the circumstances verified for the issuance of the certificate so that it is no longer in conformity with the reality.
- Any other legal cause foreseen in this CPS.

The CORPME will inform the subscriber about this circumstance prior to or simultaneously to the extinction or revocation of the validity of the electronic certificate, specifying the reasons and the date and time at which the certificate will be without effect.

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

In order to ensure the reliability and security of its operations as a Certification Services Provider, CORPME has established and implemented physical and logical security controls in all its facilities, as well as internal and independent audit procedures for monitoring and Verification of compliance with security policies, directives and procedures.

When a secure cryptographic device is required in the Provision of the Certification Service, the requirements of the ETSI EN 319 411-1 specific to NCP + (extended Normalized Certificate Policy) requirements apply.

5.1 Physical Controls

5.1.1 CORPME facilities CORPME Facilities location and physical security measures

The CORPME's technical infrastructure is located in CORPME´s Data Center, endowed with the most strict physical security measures and strict access controls to the building.

Access to the Data Center is strictly restricted and only authorized personnel can access the interior, after showing a double-factor identification: smart card and fingerprint, keeping a record of all access to data processing facilities.

Both the Data Center and the other installations and offices of CORPME Headquarters are permanently monitored from a security control with closed video surveillance circuit, motion detectors and security guards who patrol day and night the school buildings.

Areas with different levels of access and security have been defined, and it is not possible to access certain areas without an express authorization that will be reflected in the corresponding access log.

5.1.2 Physical Access

There is a complete system of physical access control of people that conform several levels of control. All sensitive operations are performed within a physically secure enclosure with varying security levels to access critical machines and applications.

The loading and unloading areas are isolated and permanently monitored by human and technical means.

5.1.3 CORPME Facilities electrical supply and environmental conditioning

CORPME's technical infrastructure is assured of operations continuity in the event of power outages, with high-capacity uninterruptible power systems and a double electrical connection with two different power suppliers.

In order to ensure the correct operation of the data processing equipment, the Data Processing center units have air conditioning units that maintain the operating temperature of the systems always within the optimum parameters.

5.1.4 Exposure to water

Adequate measures have been taken to prevent exposure to water from the equipment and wiring that make up the TSP of CORPME.

5.1.5 Measures against fires and floods

CORPME facilities have advanced fire detection, fire suppression systems, and are equipped to guarantee the tightness of the rooms containing the data processing equipment in the event of accidental or catastrophic flooding.

5.1.6 Storage System

Information related to the CORPME TSP is available on secure storage media. Storage systems are duplicated and balanced, and are located in different locations, asynchronously, to eliminate the risk associated with a single location.

5.1.7 Waste Disposal

CORPME has a waste management policy that guarantees the destruction of any material that might contain information related to its TSP, as well as a policy for the management of the removable media it uses.

5.1.8 Information Backup Policy

CORPME has defined detailed policies for the execution of the backups related to its PKI and for the maintenance of the supported information media, differentiating three methods of supporting the information according to the different assets of the CORPME TSP.

In the internal and external storage of the backup information, all legal and regulatory measures regarding data protection are applied.

5.2 Procedural Controls

For security reasons, information regarding procedural controls is considered confidential information and only part of it is included.

The TSP of CORPME seeks to ensure that all management, both operational and administrative procedures, is carried out in a safe manner, in accordance with the provisions of this document, by conducting periodic audits as set out in section 8 of this document.

CORPME ensures compliance with regulations to avoid any situation that could lead to a conflict of interest and, in this way, do not impair the fairness of operations.

CORPME subcontracts certain activities within its certification services, which are developed according the CPC and CP's and in the contracts formalized with the entities.

The CORPME TSP has an Information Security Policy that has been defined and approved by Governing Board. This policy establishes the security organization framework and, for this, it is reviewed the compliance of the operational procedures and controls related to the security in the facilities, the systems and the informative assets that provide the services.

In addition, a segregation of functions has been designed to avoid the total control of CORPME's TSP infrastructure by a single person.

5.2.1 Responsible roles for CORPME PKI control and management

The governing body, guaranteeing the principle of "minimum privilege", carries out the definition and acceptance of the responsible roles of certification services.

5.2.1.1 Management roles for hardware security modules (HSM)

- **HSM Administrator**: has the ability to perform management operations on the HSM, such as the creation and replacement of a set of cards. It is also the only one qualified to perform the FIPS140-2 Level III authorization required for critical-level operations set forth in the standard.
- **HSM Operator**: has the ability to activate (load) critical PKI keys. The activation of the keys for use is protected by a set of cryptographic cards (different from the HSM administrator).

5.2.1.2 Management roles of the CORPME PKI

The following persons are responsible for the control and management of the system:

- **Systems Administrator:** responsible for the operation of the systems that make up the PKI, the hardware and the base software. Responsibility for this profile includes, among others, the administration of the database system, the information repository and operating systems.
- **Systems Auditor:** authorized to consult and monitor the log files of the systems.
- **Security Administrator:** responsible for the management and implementation of Security Policies and Practices, established in this CPS and in the associated CP's.
- **Registry Administrator:** responsible for issuance approval, suspension and revocation of certificates.
- **Responsible of the Registry:** responsible for the processing of requests for certificates and acceptance by its subscribers of the conditions of use.

5.2.2 Number of people required per task

A minimum of two (2) people, of six (6) people, is required to perform management operations on the CORPME PKI, except for the life cycle management tasks of end entity certificates, allowed to a single Registry Operator.

5.2.3 Roles requiring segregation of functions

Between the roles, the following incompatibilities are established, so that a user cannot have two (2) roles marked as "incompatible":

- Incompatibility between the role of the System Auditor and any other role.
- Incompatibility between the administrative roles (Security Administrator and Systems Administrator, Systems Administrator and Registry Administrator).

5.3 Personnel controls

5.3.1 Requirements for professional qualification, knowledge and experience

All personnel who render their services within the scope of the CORPME TSP must have sufficient knowledge, experience and training to carry out the duties assigned to them.

To this end, CORPME will carry out the personal selection processes that it deems necessary so that the professional profile of the employee is as close as possible to specific characteristics of the tasks to be performed.

The requisite qualifications and knowledge requirements also apply whenever contracting third parties for any of the services related to the TSP.

5.3.2 Background Check Procedures

According to the personnel selection procedures established by CORPME.

5.3.3 Training requirements

According to procedures established by CORPME.

In particular, personnel related to the operation of the TSP will receive the necessary training to ensure the proper performance of their functions. The following aspects are included in the training:

- Delivery of a copy of the CPS.
- Awareness of physical, logical and technical security.
- Software and hardware operation for each specific paper.
- Security procedures for each role.
- Operating and administration procedures for each role.
- Procedures for recovery of TSP operation in case of disasters.

5.3.4 Requirements and frequency of training update

According to procedures established by CORPME.

5.3.5 Frequency and Rotation Sequence of Tasks

Not stipulated.

5.3.6 Penalties for unauthorized actions

All positions within CORPME have clearly assigned roles and responsibilities, as well as security requirements and controls applicable to each function within the organization. The safety requirements must be signed and accepted by worker, with periodic and random checks carried out by CORPME.

Failure to comply with the employee's specific safety obligations will result in disciplinary action, including dismissal, in addition to civil or criminal actions to which the seriousness and reiteration of the violations have been addressed.

CORPME will provide internal security regulations, establishing control and disciplinary mechanisms to ensure their strict compliance by employees of the service.

Among other obligations, the standards required of the staff will include the following:

- Prohibition of any use of CORPME assets and facilities to carry out illegal activities, illegal or that violate the moral and rights of third parties.
- Prohibition to dispose of any kind of information or documentation considered sensitive or confidential, as well as to transmit abroad, or to enter such information in data carriers susceptible of being extracted clandestinely from the premises of the CORPME.
- Obligation of secrecy and confidentiality with respect to the information to which the worker would have access in the performance of their duties, even after the end of the contractual relationship.
- Absolute prohibition to disclose to a third party, even within the organization itself, any password and other access data necessary to access CORPME systems and applications. The user who makes use of his access data will be personally responsible for the use made of them.
- Prohibition of any attempt to breach or attack elements or security systems, which tends to investigate access codes, regardless of the method used, or to copy, edit or delete

programs, files or information contained in other equipment located inside Of the corporate network, or outside it.

- Prohibition of corporate email abuse in non-professional uses, in particular mass mailing (SPAM) for commercial or advertising purposes.
- Prohibition of abusive use of corporate network resources for purposes not directly related to the work activity. In particular, it is expressly prohibited to use P2P (peer to peer) file download programs.
- Prohibition of the installation of any software that does not have the corresponding license of use, and of the unauthorized removal of legal software installed in the equipment of the employee, and configured by the personnel of CORPME.
- Prohibition of unauthorized access to any kind of information about natural or legal persons, as well as to incorporate personal data about such persons in automated files without the written authorization of CORPME. It is also prohibited to carry out any kind of processing on the data incorporated in the personal data files, in order to elaborate user profiles that allow inferring sensitive data that are subject to greater protection than those of which they are inferred.
- Compliance with the defined procedure for the disposal of waste, secure erasure of data carriers and destruction of obsolete or incorrect documentation, whatever its class.
- Exclusive assignment to CORPME of any intellectual, industrial and patent rights on the work, programs, developments, analyses, methodologies and in general, any product derived from the activity of the employee constant the labour relationship.

5.3.7 Requirements for contracting third parties

The general regulations of CORPME entities will be applied for contracting.

5.3.8 Documentation provided to staff

Access to the mandatory security regulations will be facilitated along with this CPS and those contained in the CP's that are applicable.

5.4 Security audit Procedures

5.4.1 Registered event types

CORPME will automatically store event-tracking information (logs) for all operations related to the systems that support your TSP activity. Measures will be taken to ensure the integrity of event logs in order to prevent any user from attempting to modify or delete the trace of actions performed on the system. Between the information of the stored events, a record of the operations related to QSCD's, such as:

- Devices' reparation.
- Registration of relevant information (sent or received) related to the registration, generation, dissemination, revocation and management of devices.

In order to ensure the detection and correction of any incidents in CORPME systems, and the debugging of errors and, where applicable, liabilities arising from use, the service logs will be subject to a strict backup and custody policy that ensures Its conservation and availability for the indicated purposes.

The synchronization period with UTC of significant environment events, key management, and revocation services is defined in a 24-hour interval.

5.4.2 Frequency of processing audit records

The records will be analysed manually when necessary, and there is no defined frequency for that process.

5.4.3 Audit records retention period

CORPME will store, during the legally established period that is, fifteen (15) years counted from the moment of its issuance, as many documents and data are necessary for the development of its activity as TSP, so that operations can be verified with them.

Licenses for use, revocation requests, certifications certifying certifiable attributes, and in general, any signed documents from which rights and obligations are derived for the participants in the CORPME TSP shall be stored for a minimum period of fifteen (15) years.

5.4.4 Audit records protection

For the archiving of electronic documents, all necessary measures will be taken to ensure the confidentiality of personal data, protection against unauthorized access, and mechanisms that ensure the integrity and absence of alterations in the stored documentation.

Periodic backups of the electronic file will be made on removable media that will be stored in CORPME security installations to ensure the recovery of file data in the event of a disaster.

Registered events are protected by encryption, so that no one, except the event display applications themselves, with their access control, can access them.

The registration services provided by external suppliers contracted by the CORPME's TSP use the registration data, previously authenticating their identity to securely exchange the information and, thus, ensure compliance with the general security and privacy requirements.

5.4.5 Procedures for supporting audit record

Backups of audit records are made according to the standard measures established by CORPME.

5.4.6 Notification to the subject causing the event

Automatic notification of the action of the audit log files to the cause of the event is not foreseen.

5.4.7 Vulnerability Analysis

CORPME has an Analysis and Risk Management Methodology, which performs risk analysis for all information assets related to the certification services' provision, assesses business requirements and determines the requirements of Security for each CP.

The risks are periodically reviewed and mitigated through a Treatment Plan. Safelayer's KeyOne technology has mechanisms to check the binary integrity files and the operation of certificate management systems.

5.5 Archiving records

5.5.1 Archived events types

CORPME will keep a file with the following documents and files related to its activity of Certification Services Provider.

- Documentation related to the generation protocols and conservation of Main Keys of the Service: Root, Internal, and External Certification Authorities.
- List of revoked digital certificates (CRL's and ARL's).
- Logs and records of service incidents.
- Applications for issuance, revocation and licenses of use of Certificates.
- Documentation certifying certifiable attributes.
- Version history of the CPS and CP's.

5.5.2 Record retention period

CORPME will store, during the legally established period that is, fifteen (15) years counted from the moment of its issuance, as many documents and data are necessary for the development of its activity as Certification Services Provider so that operations can be verified with them.

5.5.3 File Protection

The log files are protected by encryption, so that nobody, except the display applications themselves, with their access control, can access them.

5.5.4 File Backup Procedures

File backups are performed according to CORPME's associated internal procedure.

5.5.5 Requirements for time stamping of records

The information systems used by the CORPME TSP guarantee the time registration in which they are made. The instant of time of the systems comes from safe source of ROA that verifies the date and hour. All systems are synchronized with this official source.

The synchronization period with UTC of significant environment events, key management, and revocation services is defined in a 24-hour interval.

5.5.6 File information system (internal vs. External)

The TSP audit information system is a combination of automatic and manual processes executed by the available applications.

5.5.7 Procedures for obtaining and verifying archived information

Registered events are protected against unauthorized manipulation. Only authorized personnel have access to the physical media files and computer files, to carry out integrity checks or other tasks as appropriate.

5.6 Change of keys

The procedures for providing, in the event of a change of keys, a new CA public key to the subscribers and third party acceptors of the CA's certificates are the same as to provide the current public key. Consequently, the new key will be published in the CORPME TSP repository.

5.7 Recovery from key or catastrophic commitment

The CORPME's TSP has developed and approved a Business Continuity Plan that contemplates the procedure of action against a signature creation data vulnerability, aimed at solving the incident as soon as possible. This procedure is based on the realization of a series of actions for the management of the crisis as an integral part of the plan:

- Stop the provision of the affected service.
- Revoke the affected certificates.
- Execute relevant communications to affected parties, including information on the compromise produced.
- Study the need to activate the Plan for Completion of TSP activities.

5.7.1 Incident and commitment management procedures

CORPME has established a security plan that defines the actions to be taken, resources to be used and personnel to be employed in the event of an intentional or accidental event that depletes or degrades the resources and services of CORPME TSP.

In the event of a compromise of the signature verification data of any Certification Authority, CORPME shall inform all CORPME certificate holders and known third party acceptors that not all certificates and revocation lists signed with these data already are valid. As soon as possible, the service will be restored.

5.7.2 Alteration of hardware, software and / or data resources

If hardware, software, and / or data is altered or suspected to have been altered, operation of TSP will be stopped until the security of the environment is restored with the incorporation of new components whose adequacy can be accredited. Simultaneously an audit will be carried out to identify the cause of the alteration and ensure its non-reproduction.

In the event of the loss of calibration of a clock with the UTC, time stamp service will be recovered as soon as possible, as established in the Continuity Plan.

In case of being affected certificates issued, users will be notified of the fact and a new certification will be carried out.

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

In the event of compromise of private key of the CA, it will proceed to immediate revocation. Next, the corresponding CRL will be generated and published, ceasing the operation of the CA activity and proceeding to the generation, certification and start-up of a new Authority with the same name as the one eliminated and with a new key pair.

In the case of CA, the revoked certificate thereof will remain accessible in the repository of the CORPME TSP in order to continue verifying the certificates issued during its period of operation.

All affected parties will be notified that certificates and information about their revocation, supplied with the compromised key of the CA, cease to be valid from the moment of notification, and must use to verify the validity of information the new public key of the CA.

5.7.4 Installation after a natural disaster or other catastrophe

The system of Certification Authorities of CORPME TSP can be rebuilt in case of disaster. To carry out this reconstruction it is necessary to have:

- A system with hardware, software and Cryptographic Security Device similar to the one existing prior to the disaster.
- The CA administrator cards.
- A backup of the disks of the pre-disaster system.

With these elements, it is possible to rebuild the system as it was at the time of the backup made and thus recover the CA, including its private keys.

Backups are performed periodically and backup and restore functions are performed by Trusted Roles, applying the necessary controls to ensure the recovery of essential information and software.

The storage of both CA administrator access cards and copies of CA system disks is carried out in a different place, sufficiently remote and protected to make it difficult to concurrently simultaneous catastrophes in production systems and recovery elements.

5.8 CA or RA Termination

CORPME will cease its activity as TSP, by virtue of the dissolution agreement adopted by the Assembly of Territorial and Autonomous Deans, by a law that establishes it or by a firm judicial decision.

5.8.1 CA Termination

In case of termination of the CA, the CORPME:

- Ensure that the potential problems for subscribers and third party acceptors are the minimum, as well as the maintenance of registry required to provide truthful proof of certification service for legal purposes.
- Communicate any relevant circumstances that may prevent the continuation of its activity in the CA.
- It will notify its intention to cease activity of CA as a PSC to the holders of its certificates, users or any entity who has a contractual relationship of certificate use of, by any means that guarantees sending and receipt of the notification and with a minimum notice period of two (2) months, or the period established by current legislation.
- Keep the active certificates and the system of verification and revocation until the extinction of all certificates issued.
- Process the revocation of the certificate of affected CA's.
- Destroy or disable CA private keys, including backup copies, co that they can not be recovered.
- Send to the Ministry of Energy, Tourism and Digital Agenda prior to the definitive cessation of its activity the information related to certificates whose validity has been extinguished for the latter to take care of their custody.

In case of the transfer the activity to other CA, the CORPME:

- It will send the transfer agreements and a document explaining the conditions that will govern the relations between the subscriber and the PSC where the certificates are transferred. This communication will be made by any means that guarantees the sending and receipt of the notification, at least two (2) months before the end of its activity, or the period established by the legislation in force.
- Transfer, with subscribers express consent and with strict all the guarantees regarding personal data protection observance, those certificates that remain valid on the effective cessation activity date, as well as rights and obligations arising of the same and the information and documentation related to all issued certificates, to another TSP that guarantees similar levels of security and reliability in its procedures. If this transfer is not possible, certificates will be revoked.
- It will revoke the certificates after a period of two (2) months, or the period established by the legislation in force, provided that there is no transfer agreement or without the express

consent of the subscriber, who must also accept the terms of the agreement. PSC to which they are transferred.

5.8.2 RA Termination

In case of termination of RA, the CORPME will:

- Transfer to the designated entity, during the 24 hours following the cessation, the registers they maintain as long as there is an obligation to keep the information archived. Otherwise, the records will be destroyed.
- Carry out the necessary actions to transfer its obligations regarding the maintenance of the registry information and of the logs during the indicated time period to the subscribers and users that trust.

6 TECHNICAL SECURITY CONTROLS

In addition to the physical security controls established at CORPME's facilities, and the security measures implemented to protect the data used to provide the Certification Service, CORPME will submit its activity to the strictest technical security controls that Ensure compliance with the highest standards of quality and reliability, in accordance with applicable regulations and technical and market standards.

6.1 Generating and Installing the Key Pair

6.1.1 Generation of the key pair

Both the Root Certificate and CORPME Internal and External certification authorities' secondary keys have been generated following the procedures and formalities defined in the Key Ceremony prior to the start of the TSP activity, with the personal intervention of the Director of the Service, and the presence of members of the Governing Board as witnesses to the act of generation.

The Service Keys have been generated directly inside a secure cryptographic device, certified as FIPS 140-2 level 3, using RSA algorithms with a key length of 2048 bits, and 4096 bits in the case of the Root CA and Subordinated.

The custody of the signature data of the Root and Subordinated CA is the Director of the Service, the device containing the keys in a safe of high security.

The period of validity of the service keys has been restricted for security reasons to a maximum of twelve (12) years, even though the standards allow a higher validity that can reach twenty (20) years.

CORPME, once the validity period of the Service Keys (Root and Secondary) has expired, will securely store the same, in order to prevent its subsequent use. Proceeding, in accordance with the protocols defined for the Ceremony of Keys, to the generation of some new keys of the Service.

The key pairs for the other holders are generated according to the provisions of the CP applicable to each certificate.

The hardware or software devices to be used in the generation of keys for each type of certificate issued by the CORPME TSP are defined by the CP applicable to it.

6.1.2 Delivery of the private key to the holder

The owner himself in his cryptographic device generates the private key of the certificates, so that, in no case, the distribution of the device and the generation of the private key pose a security risk relative to the delivery itself.

The signature creation cryptographic device is stored securely and distributed directly to the holder to avoid possible incidents in sending and receiving.

6.1.3 Delivery of the public key to the certificate issuer

The public key of the certificates is generated in the owner's own secure cryptographic device.

6.1.4 Delivery of the CA public key to trusted third parties

Both the Primary Key and Root of the Service and those corresponding to the subordinate certification authorities of the Internal and External Secondary Key will be permanently available for download from CORPME´s portal website (http://pki.registradores.org/normativa/index.htm).

6.1.5 Key length

The size of the keys used is:

- 4096 bits for the CORPME Root Certification Authority.
- 4096 bits for CA Internal Certificates and CA External Certificates.
- 2048 bits for the Time Stamping Authority.

The CP as the sea of application defines the size of the keys for each type of certificate issued by the CORPME TSP.

6.1.6 Public Key Generation Parameters and Quality Verification

The period of use of the private key will generally be the same as the period of validity of the certificate. Notwithstanding the foregoing, and with reflection in the corresponding CP, it may be established by introducing an extension within the X509 v.3 standard, a private key use period that is shorter than certificate validity, in those Cases in which the representation or attribute certified by the subscriber has a known expiration and before the expiration of the certificate itself. In these cases, the validity period of the certificate will be limited to the validity of the certificate, which is, to the validity of the represented attribute.

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

The CP applicable to it defines the accepted uses of the key for each type of certificate issued by the CORPME TSP.

All certificates issued by the CORPME TSP contain the Key Usage extension defined by the X.509 v3 standard, which qualifies as critical. Additional limitations may be set using the Extended Key Usage extension.

6.2 Private Key protection and engineering controls for modules

6.2.1 Standards for Cryptographic Modules

The cryptographic modules used in the CORPME TSP for the creation of used keys comply with FIPS 140-2 level 3 certification.

The implementation of each of the Certification Authorities carries out the following tasks:

- Initializing the status of the HSM module.
- Creation of the keys of the
    - HSM Administrators.
    - HSM Operators.
    - Security Administrators.
    - Systems Administrators.

- Registry Administrators.
- Systems Auditors.

- Generation of CA keys.

The CORPME TSP uses commercially available hardware and software cryptographic modules developed by third parties.

The controls related to the use, configuration and correct operation of the cryptographic modules are detailed in the HSM Life Cycle Procedure.

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

The private key of CORPME TSP CA's is under multi-person control. This is activated only by initializing the CA software by means of the minimum combination of the corresponding CA operators.

Two (2) CORPME HSM Administrators are required, out of a total of six (6), to enable one (1) of the five (5) HSM Operators to subsequently activate and use the CA private key.

6.2.3 Private Key Custody

The private keys of the Certification Authorities that make up the CORPME TSP are housed in secure cryptographic hardware devices and have FIPS-2 level 3 certification associated with the different CA's, using RSA algorithms with a key length of:

- 4096 bits for Subordinate CA's.
- 4096 bits for the Root CA.

6.2.4 Private Key Backup

The private keys of CORPME TSP CA's are stored on secure cryptographic devices with similar characteristics to HSM and only CA Root operators have access.

6.2.5 Archiving the Private Key

The private keys of the users will never be archived one ends its period of validity to guarantee the non-repudiation.

6.2.6 Transferring the Private Key to/or from the Cryptographic Module

The transfer of the private key is performed between cryptographic modules (HSM) and requires the intervention of at least two (2) of the six (6) HSM Administrators and one (1) of the five HSM for later activation.

6.2.7 Storing Private Key in a Cryptographic Module

The private keys are generated in the secure cryptographic module at the time of creation of each of the CORPME TSP Authorities. Each of these Authorities makes use of these modules and is kept encrypted.

The private key security in the cryptographic module is guaranteed by means of preventive measures that avoid the manipulation of the stored device.

6.2.8 Method for activating the private key

As stated in section 6.2.2 of this document, the private key of CORPME TSPs CA's is activated by initializing the CA software by means of the minimum combination of the corresponding CA operators (Administrators and Operators).

Specifically, two (2) HSP Administrators of the CORPME PKI, of a total of six (6), are required to enable one (1) of the five (5) HSM Operators to activate and use the private key Of the CA's.

6.2.9 Method for deactivating the private key

The HSM Administrators, in combination with the HSM Operators, may deactivate the CORPME TSP Certification Authorities key by stopping the corresponding CA computer application.

6.2.10 Private Key Destruction Method

Not stipulated.

6.2.11 Cryptographic Modules Classification

The cryptographic modules used are certified and meet FIPS 140-2 level 3 standard.

6.3 Other aspects of Key Pair management

6.3.1 Public Key File

Subscriber Signature Verification Data will be archived in case it is necessary to retrieve it, in secure files and media, both physically and logically, during the legally established period of fifteen (15) years.

6.3.2 Certificate operative periods and Key Pair usage period

The certificate and key pair of the Certification Authority of CORPME are valid for twenty-four (24) years and those of the CA's of External Certificates and CA of Internal Certificates of twelve (12) years.

The corresponding CP will establish the period of validity of the remaining certificates.

6.4 Activation Data

6.4.1 Generation and Installation of Activation Data

For the creation of the Certification Authority, cryptographic cards must be created, which will be used for recovery and operation activities. The following are the roles used in the CORPME CA, each with its corresponding cryptographic cards:

- HSM Administrator Cards.
- HSM Operator Cards.
- Security Administrators Cards.
- System Administrators Cards.

- System Audit Cards.
- Registry Administrators Cards.

If one or more cards are lost or damaged, or the administrator forgets his PIN or is no longer usable for any reason, the entire set of cards should be rebuilt as soon as possible using all of the distributed security cards.

6.4.2 Activation data protection

Only authorized personnel, in this case the partition operators corresponding to each CA, have the cryptographic cards that can activate the CA's and know the PINs and passwords to access the activation data.

By establishing multi-person control, without the prior intervention of the HSM Administrators, the HSM Operators will not be able to carry out the activation of the CA's by themselves.

6.4.3 Other aspects of activation data

Not stipulated.

6.5 Computer Security Controls

The data related to this section is considered as a confidential information and will only be provided to those who justify the need to know them, as in the case of external or internal audits and inspections.

The TSP of CORPME applies the measures of computer security related to:

- Perimeter and network security, to protect the domains of the internal network of the TSP against unauthorized access. Continuous monitoring and alarm services are provided to detect record and react in a timely manner to any unauthorized access to your resources.
- User management, to manage the registration, registration and modification of user accounts.
- Access control policy, including separation of security management and operation functions. The broadcast application complies with access control in attempts to add or remove certificates and modify other associated information. The revocation status application enforces access control in attempts to modify revocation status information.
- User identification and authentication, to use critical applications. Multifactor authentication applies to all accounts that are capable of directly issuing a certificate.

CORPME maintains the components of the TSP's local network in a physically and logically safe environment, and the configurations of these components are periodically reviewed to verify compliance with the established requirements.

6.5.1 Specific technical security requirements

The data related to this section are considered confidential information and will only be provided to those who prove the need to know them, as in the case of external or internal audits and inspections.

6.5.2 Computer security assesment

The CORPME TSP periodically evaluates its level of security in order to identify possible weaknesses and establish corresponding corrective actions through external or internal audits and inspections, as well as the continuous implementation of security controls.

6.6 Lifecycle Security Controls

The data related to this section are considered confidential information and will only be provided to those who justify the need to know them, as in the case of external or internal audits and inspections.

The CORPME TSP applies life-cycle safety measures related to:

- Change management, to manage new projects, evolutionary and software corrections.
- Malicious software control, to protect the system integrity against viruses or malicious software.
- Management of media, against storage media obsolescence and deterioration.
- Control of updates and security patches, against vulnerabilities in the system.

6.6.1 System Development Controls

The data related to this section are considered confidential information and will only be provided to those who prove the need to know them, as in the case of external or internal audits and inspections. These controls are required from outset, both in the acquisition of computer systems, and in development of them.

6.6.2 Security Management Controls

CORPME's TSP maintains an all IT assets inventory and performs its classification according to protection needs it has defined, in line with its risk analysis.

The TSP of the CORPME carries out periodic capacity requirements checks. Due to this, a Capacity Plan is available to monitor and project future infrastructure capacity requirements, ensuring a degree of availability and services occupation, and identifying future investments to maintain the capacity of processing and storage of services.

The configuration of the systems is audited periodically.

6.6.3 Lifecycle Security Controls

There are security controls throughout the life cycle of the systems in the CORPME TSP.

6.7 Network Security Controls

The data related to this section are considered confidential information and will only be provided to those who prove the need to know them, as in the case of external or internal audits and inspections.

CORPME performs reliable vulnerability analysis and penetration testing in systems to improve safety.

The TSP of CORPME applies the security measures of the network related to:

- Segmentation of their systems in networks, considering the functional, logical and physical relationship between systems and services. A bastion is performed of the CA

equipment is performed, disabling all users, applications, services, protocols and ports that are not used in CA operations.

- Security in communications, through secure channels logically different from other communication channels. There are security procedures for system and communications protection, which keep CA systems in a secure network zone.
- Accessibility in high security areas, for the unique access of the Trusted Roles.
- Availability of network services.

6.8 Time Stamping

Timestamping is an on-line mechanism that allows to demonstrate that a data series have existed and have not been altered from a specific time in time.

CORPME is a Time Stamping Authority (TSA or Timestamp Authority) that acts as a trusted third party testifying the existence of such electronic data at a specific date and time.

The timestamping Policy of the Registrar's Office will establish the obligations and responsibilities, as well as the operational requirements during the time stamp.

7 CERTIFICATES, CRL AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version Number

All certificates issued by CORPME comply with version 3 of the X.509 standard, allowing the inclusion of extensions for certification of attributes.

7.1.2 Certificate extensions

The extensions used generically in certificates are:

- *Subject Key Identifier.*
- *Certificate Policies.*
- *Basic Constraints.*
- *Key Usage.*
- *Thumbprint Algorithm.*
- *Thumbprint.*

The CP's of CORPME's TSP can establish joint variations of the extensions used by each type of certificate.

The CORPME TSP has defined an OID allocation policy within its private numbering range by which the OID of all CORPME Proprietary Extensions of Certificates begins with the prefix 1.3.6.1.4.1.17276.0.

7.1.3 Object identifiers (OID) of algorithms

Object Identifier (OID) of Cryptographic algorithms: SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

7.1.4 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).

7.1.5 Name Restrictions

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

7.1.6 Certification Policy Object Identifier (OID)

Each of the CP's will define its own object ID (OID).

The TSP of CORPME has defined an OID allocation policy within its private numbering range by which the OID of all CP's of the CORPME TSP starts with the prefix 1.3.6.1.4.1.17276.0.

7.1.7 Using the extension "PolicyConstraints"

Not stipulated.

7.1.8 Syntax of the "PolicyQualifier"

The Certificate Policies extension contains the following Policy Qualifiers:

- CPS: contains the URL that collects the CPS and the CP's that govern the certificate.
- Notice Reference: Text note that is displayed on the screen, at the instance of an application or person, when a third party verifies the certificate.

7.1.9 Semantic processing for critical extension "Certificate Policy"

If it is desired to maintain the maximum capacity to be able to operate with other CA's of the certificate, the extension will be classified as *noncritical*. This is done following the recommendations for standard S / MIME secure email applications [RFC5750] and SSL / TLS web authentication [RFC5246]. Applications may use the information contained in that extension, even though it is a non-critical extension.

7.2 CRL Profile

7.2.1 Version Number

The Directory is published in accordance with the Lightweight Directory Access Protocol (LDAP) standard and certificate revocation lists according to the X.509 standard Certificate Revocation List (version 2). The OCSP (On-line Certificate Status Protocol) standard may also be used.

7.2.2 CRL and extensions

Not stipulated.

7.3 OCSP Profile

7.3.1 Version Number(s)

In addition to the publication of the CRLs, the TSP 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. The URLs for access to the OCSP service are as follows: **http://ocsp.registradores.org** and **https://ocsp.registradores.org**

7.3.2 OCSP Extension

The Validation Authority supports:

- Petitions signed.
- Extension NONCE.

8 COMPLIANCE AUDITS AND OTHER CONTROLS

8.1 Frequency of circumstances of controls for each Authority

On a regular basis and in order to verify effective measures implementation contained in the CPS and CP's, the Safety Officer will order and supervise the performance of internal and independent audits.

In addition, CORPME's TSP will be able to carry out audits to the different Processing Units, to guarantee the life cycle of the certificates and to supervise the associated procedures.

8.2 Identification / Qualification of the Auditor

Qualified and independent personnel carried out by experts of recognized prestige will carry out the Internal Audits.

8.3 Relationship between the Auditor and Audited Authority

In order to avoid a conflict of interest, the external auditor and the audited party should not have any relation, apart from the audit function.

8.4 Aspects covered by controls

The audit will determine the adequacy of CORPME TSP services with this CPS and applicable CP's. It will also determine the risks of breach of adequacy with the operations defined by those documents.

The scope of activity of an audit shall include at least:

- Security and privacy policy.
- Physical security.
- Technology Assessment.
- Administration of CA services.
- Recruitment.
- CPS and competent CP's.
- Contracts.

8.5 Actions to be taken as a result of deficiencies detection

The identification of deficiencies detected because of the audit will lead to corrective action. The Policy Approval Authority (PAA), in collaboration with the auditor, will be responsible for determining the same.

In case of serious deficiencies, the Policy Approval Authority may adopt, among others, the following decisions: temporary suspension of operations until deficiencies are corrected, revocation of the Authority's certificate, changes in personnel involved, invocation of the most frequent global responsibility and audit policy.

8.6 Communication of results

Although the result of the same is confidential information, deficiencies detected in the development of such audit would be rectified in the shortest possible time whenever they are anomalies of CORPME.

9 OTHER LEGAL AND ACTIVITY ISSUES

9.1 Rates

9.1.1 Certificate or renewal rates

The issuance of foreign key certificates will be made free of charge for all individuals requesting a personal certificate, as well as for the other applicants for foreign key certificates.

Whenever for security reasons and for setting up a Qualified Electronic Signature, Qualified Certificates are generated directly within a QSCD, and in no case are issued in software, the applicant must obtain as a prerequisite to the issuance of its certificate, and at its expense, a signature Creation Device approved by CORPME. In the Processing Units, "Electronic Signature Kits" will be available to interested applicants, including a QSCD, as well as the licensed software required for the use of the certificate.

The queries related to the price applicable to the signature kits, and the conditions for the payment of the same, will be met upon request in which the interested party should contact CORPME through the email address: **psc@registradores.org**.

9.1.2 Certificate access fees

The queries related to the access fees to the CORPME TSP certificates will be met upon request, in which the interested party should contact CORPME via email: **psc@registradores.org**.

9.1.3 Access fees to the information status or revocation

The queries related to the fees for accessing the status information or revocation of the CORPME TSP certificates will be met upon request, in which the interested party should contact CORPME via email **psc@registradores.org**.

9.1.4 Other service rates

The queries related to the fees of any other services of CORPME´s TSP certificates will be met upon request, in which the interested party should contact CORPME via e-mail: **psc@registradores.org**.

9.1.5 Refund Policy

Consultations related to the policy of reimbursement of the TSP of CORPME, will be met on demand in which the interested party should address to CORPME via email: **psc@registradores.org**.

9.2 Economic Responsibilities

CORPME has the necessary financial solvency to meet the responsibilities that the current legislation requires it to assume. Insurance instruments approved by Law 59/2003, for the legally established amount of THREE MILLION EUROS (€ 3,000,000), cover these liabilities.

The CP's applicable to each type of certificate shall establish the maximum amount up to which CORPME's liability for damages will be extended to subscribers and third parties.

9.2.1 Indemnification of CA's and/or RA's

Not stipulated.

9.2.2 Fiduciary relationships between various entities

Not stipulated.

9.2.3 Administrative procedures

Not stipulated.

9.3 Confidentiality of information

Regardless of the provisions of Article 6 of Royal Decree-Law 1298/1986 of 26 June, on the duty of confidentiality of data and information available to CORPME in the exercise of its functions, the following is established: Confidentiality of data relating to the TSP of CORPME.

9.3.1 Confidential information scopes

All information generated by CORPME TSP that is not stipulated as a publication will be considered as confidential. The following is expressly determined as confidential information:

- Private keys of the Authorities that make up the TSP of CORPME.
- Information on the operations carried out by CORPME TSP.
- The information related to the parameters of security, control and audit procedures.
- The personal information provided by the certificate subscribers to the CORPME TSP during the registration process, in accordance with the regulations on the protection of personal data and rules of development.

9.3.2 Non confidential information

It is considered public information and therefore accessible by third parties:

- The one contained in this document.
- The one included in the CP's that apply to it.
- Certificates issued by the TSP of CORPME.
- The list of suspended or revoked certificates (CRLs).

9.3.3 Professional Secrecy Duty

All employees of CORPME who are involved in any of their own tasks or derived from their TSP are bound to the duty of professional secrecy. The contracted personnel that participate in any activity or operation of the TSP of CORPME is also subject to the secrecy duty in the framework of the contractual obligations contracted with CORPME.

9.4 Personal Information Protection

9.4.1 Applicable legal framework

CORPME's policy on the personal data protection will be developed in accordance with the national and Community regulations in force in the matter:

- Organic Law 15/1999 of December 13, on Protection of Personal Data.
- Royal Decree 1720/2007 of 21 November, which regulates the security measures of automated files containing personal data.
- Directive 95/46 / EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 97/66 / EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

9.4.2 Data Protection applicable to CORPME´s activity

CORPME will protect the Files containing Personal Data in accordance with the provisions of current legislation, in particular LOPD 15/1999, and Regulation 1720/2007.

Except for Registrar Qualified Certificates and Legal Person Representative Qualified Certificates, as long as these contain corporate information that may be published in the Business Registry, the data files used in the management of the certification service shall be private. The data used in the Public Registers and that under the CP's are incorporated in the CORPME certificates, will be treated in strict accordance with the Data Protection policy of the Association of Registrars of Spain, holder of the Data Files that Contain information on companies and their representatives.

CORPME will be in respect of the data contained in the public files of commercial information, responsible only for its treatment, which will be carried out in accordance with the guarantees defined in the current legislation.

The creation, alteration and destruction of files containing personal data will be timely notified to the General Registry of Data Protection, put in charge of the Spanish Agency for Data Protection.

Ownership of the personal data files collected during the provision of the Certification Service will be owned by CORPME who will proceed to its registration and maintenance in accordance with the applicable regime.

The Registration Units located in the Business Registers and other registration points that Registrar may authorize with CORPME Governors Board agreement, as soon as they have access to documents and personal certificates applicants and subscribers data, for their duties performance, shall bear in respect of said data consideration of those responsible for their treatment, which in accordance with LOPD article 12, to what is established below. In addition, the *Processing Units*, in compliance with what is established in articles 7, 9 and 12 of the LOPD, undertake to:

- To access files and personal data whose ownership corresponds to CORPME, only to the extent that such data are necessary for its activity as Registry Authority, and consequently give them the appropriate use excluding any other.
- To make access to data and its treatment, in accordance with the provisions of this CP, the TSP's internal regulations, and the instructions received from the Steering Committee.
- Not to disclose personal data to which they had access during the performance of their duties, as well as to protect the right to honour and privacy of those affected.
- To adopt and comply with the necessary technical and organizational measures to guarantee the *security of the Systems, Files, people and processes* in which access or processing of Personal Data is made. These measures will be reflected in the security document defined in the Royal Decree of Security Measures 1720/2007.
- To use in its communication with CORPME only secure communication channels protected by encryption, as well as the authentication mechanisms necessary to ensure the confidentiality of the transmissions.
- To return or remove, in accordance with the instructions received from the person responsible for the File, the personal data of which it was in possession at the end of the relationship with CORPME, in case that by decision of the CORPME Governing Board, Executed by the Steering Committee, in accordance with the Regulation of the Service, some Processing Unit will cease to be.

- To request from Applicants and Subscribers of certificates, in the processes before the Processing Unit, the express consent for the processing of their personal data, as it is necessary for the provision of the Certification Service. Keeping record of such consent to the appropriate effects. In any case, and without prejudice to the express authorizations that may be requested from the affected party in forms and documents of the Service, it is presumed, as essential for the provision of the requested Certification Service, that the applicant or the subscriber consents to The processing of your personal data, only as it relates to the provision of such service.

The communication to third parties that rely on digital certificates issued by CORPME of the personal data incorporated in said certificates, and that they are published in the Directory of Certificates of CORPME. It will be carried out in accordance with the provisions of Article 11 of the LOPD. In this sense, the Subscriber consents, as a budget for the legal effectiveness of the certification service provided by CORPME, the publication in the Certificate Directory of the personal data associated with the public key of the certificate, which constitutes for any third party the medium of verification of the signature of the subscriber.

Access to the information contained in the Agenda application, which manages appointments for the issuance and renewal of certificates in the Processing Units, and in the Revocation Lists may be made by third parties in good faith, only to the indicated verification effects Of the electronic signature of the subscriber, prohibiting any access to said data and its compilation for further processing and use for purposes other than those described. Violations consisting of data dump, and subsequent processing and use for purposes other than those authorized, will be punishable by a fine of up to 600,000 euros, and may result in criminal and civil actions.

In any case, the Applicants and Subscribers of Digital Certificates of CORPME are guaranteed the free exercise of the Access, Rectification, Cancellation and Opposition rights, provided for in the LOPD. The affected party should address his request to CORPME in writing to the postal address of the Service that appears in the corresponding section of this CPS.

9.4.3 Security Document

9.4.3.1 Definition and scope of CORPME´s Security Document

CORPME and for the sole purpose of providing the Certification Service, collect during the applicant's registration process of the applicant in the agenda: (**https://www.registradores.org/scr/agenda**), or during the issuance process Of certificates in the personal appearance of the applicant before the Processing Unit, certain personal data of the Requesters and Subscribers.

Because of the access and treatment that it performs of the personal data of the applicants and subscribers, for the provision of the Certification Service, CORPME must adopt the security measures required in accordance with the provisions of Royal Decree 1720/2007, elaborating a security document for this purpose.

The security document defines and regulates the application of the organizational and technical measures that guarantee the security of the data incorporated in the data files of which CORPME is responsible. Providing what is necessary for their preservation, safeguarding their integrity, confidentiality and legitimate use according to the purpose for which they were collected.

The measures applicable under the Security Document will be extended to the different areas of activity of CORPME as a Certification Authority that issues Qualified Digital Certificates, as well as to the Processing Units that, in accordance with Regulation 1720/2007 and this Certification Practice Statement to develop Registry Authority functions.

All employees of CORPME who have any direct or indirect, regular or incidental contact with personal data, or who participate in any way in their treatment, shall be bound by the policies and controls defined in the Security. Each employee shall be notified in writing of the scope of his / her responsibilities for data protection, as well as the procedures and controls applicable to him depending on his position within the organization. The employee will sign at the receipt of the security documentation a document that accredits his knowledge and acceptance of the aforementioned obligations and responsibilities that he assumes.

The CORPME Security document has the following content:

- **General Security Guidelines,** which lists the general security guidelines to be implemented for activities related to the safeguard and security of Automated Files with Personal Data.
- **Security Organization,** where it is structured and dimensioned security organization that CORPME establishes to safeguard and ensure the confidentiality of all personal data it handles.
- **Information Systems,** where they identify and describe the Information Systems dependent on CORPME through which a processing of Personal Data is performed.
- **Rules and Procedures,** which define and describe a set of necessary and obligatory Norms and Procedures to safeguard the information and ensure the confidentiality of the Personal Data of the CORPME Information Systems

9.4.3.2 Roles in policy enforcement and data protection

The body responsible for defining and implementing security policies is the CORPME Safety Committee, which is constituted by:

- The CORPME Information Systems Officer.
- Responsible for Security LOPD of CORPME.
- The Operators of Exploitation of CORPME facilities.
- The departmental responsible of files with Personal Data (hereinafter PD).

Also participating in the Security Committee will be the Registrars who are members of the work commissions of CORPME, in the areas of affinity to Data Protection.

The functions of the Security Committee shall be, inter alia, the following:

- Study and analysis of security strategies.
- Designate the Security Officer of CORPME to coordinate and control the implementation of the security measures, standards and procedures defined in this Security Document. The Security Officer, once appointed, will become a member of the Security Committee.
- Analysis of the proposals for modification of the Security Document prepared by the Security Officer.
- Analysis of the corrective measures to be implemented derived from the audit reports that are carried out periodically in matters of security of Personal Data.
- Review of verification reports of correct compliance with the provisions of the LOPD Security Document, issued by the Security Officer.
- Analysis of the explanatory reports of those incidents that seriously affect the Information Systems, issued by the Security Officer.
- Monitoring of the different Security Plans that are defined.
- Discuss any other topic that is considered of interest in computer security.

Without prejudice to the maximum responsibility for data protection held by the Security Committee, they shall be responsible for the implementation of the measures covered by the security document, within the scope of their respective functions, the File Manager and the Security Officer.

9.4.3.2.1 File manager

CORPME will be responsible for the files of personal data that in the performance of their duties as a Trust Service Provider, have access. The person in charge of each department in which security measures and controls are to be implemented in accordance with the security document will perform the functions that Regulation 1720/2007 puts in charge of the File Manager. The functions of the File Manager are, among others, the following:

- Elaborate and implement the Security Document of the automated files containing PD within the scope of their respective department.
- Adopt the necessary measures so that personnel accessing the Information Systems with PD know the security rules that affect the development of their functions, as well as the consequences that can be incurred in case of non-compliance. This task is done in collaboration with the Security Officer.
- Authorize in writing the execution of the processes of recovery of PD, as established in the Procedure of Recovery of Personal Data.
- Establish the criteria to be followed when granting, altering or cancelling authorized access of users to the Information Systems handling PD in CORPME.
- Authorize the release of computer media containing Personal Data outside the premises where the file is located, according to the Procedures for Exiting Computer Media with Personal Data.
- Authorize the use of real PD in the tests of the applications that handle the files with PD.
- Adopt appropriate corrective measures to address the security deficiencies of PD that are detected after regular, internal, and independent audits to be carried out.
- Authorize the access, modification and deletion of PD, requested by the data holders as described in the Procedure for Execution of Rights of Access, Modification and Suppression of PD.
- If applicable, include in clauses establishing the obligations of the company providing the service with respect to the security of the PD it handles in contracts for the provision of services involving access to PD.

9.4.3.2.2 Security Responsible

The Security Officer coordinates and controls all the tasks and activities that are carried out in the security field of DP in CORPME. It is also responsible for the definition, implementation and supervision of the Norms and Procedures that affect the files with DP.

The functions assigned to the Security Officer of CORPME are as follows:

- Notify for registration in the general data protection registry, the creation and modification of automated files containing personal data.
- Maintain updated the Inventory of Files with personal data.
- Collaborate with the File Manager in defining a collection of user profiles, specifying the access options allowed and the type of access required (update or query) to the applications that deal with the files.
- To specify the technical and administrative data to fulfil the requests of user administration derived from the needs expressed by the Responsible of the User Areas.
- Authorize the subscriptions, un-subscriptions and modifications of access of the users to the Information Systems that handle DP, following the criteria determined by the File Manager.
- Process the user request by means of the enabled mechanism of identified update and access password.
- In the issuance of Personal Data from CORPME, request from the File Manager, the mandatory authorization for the output of media containing personal data.
- Participate in the recovery processes of DP, as established in the Procedure of Backups and Data Recovery:
    - Verify the definition and application of the Procedure of realization of Copies of Backup and Data Recovery.

  - Communicate to the File Manager the need for data recovery in order to obtain authorization for the same.
  - Participate in the decision-making associated with data recovery.
- Advice, in the definition of requirements, on the security measures to be taken in the development of applications that handle DP. Validate that the necessary security requirements have been implemented.
- Up-to-date maintenance of the LOPD Safety Document:
  - Define and establish the Norms and Procedures that in security matters affect the automated files with DP.
  - Keep updated the Norms and Procedures that in security matters affect the files automated with DP.
  - Keep updated in the scope of the Security Document the information related to Information Systems containing DP.
  - To be informed of the changes that may occur in the legal provisions on the processing of Personal Data, and propose measures of adequacy to such changes, and in particular changes that alter the Security Document.
- Verification of compliance with the provisions of the LOPD Security Document:
  - Periodically verify, according to the Regulations to regulate the periodic controls to verify the provisions of Regulation 1720/2007, the correct compliance with the actions that in terms of security of DP are carried out in CORPME.
  - Prepare reports to verify compliance with the provisions of the CORPME Security Document and present them, if it deems appropriate, to the Security Commission.
  - Creation, modification and deletion of files
  - Prepare the publication provisions in the BOE of the creation, modification or deletion of CORPME files containing DP and are publicly owned.
  - Periodically check the consistency of the information contained in the Inventory of Files with DP with that existing in the LOPD Security Document.
- Collaboration in Security Audits:
  - Check that the LOPD Security Audit is carried out at least every two years for medium and high level files, if any.
  - Transfer the audit reports that are periodically made to the File Manager.
  - Analyse the Audit reports and if necessary, raise the corrective measures to be implemented by the Security Commission for approval.
- Security Management of Information Systems:
  - Monitor and keep up-to-date records of users with authorized access to information systems.
  - Supervise and analyse the security incidents occurring in CORPME in relation to the security of automated files with DP.
  - To dictate measures whose application minimizes and / or eliminates incidents. O Periodically review the control information recorded on the user's access to the Information Systems (LOG traces) and periodically (at least once a month) prepare a report of the revisions made and the problems detected. O Meetings of the Security Commission:
    - Attend and participate in the meetings of the Security Commission.
    - To present the proposals that it deems necessary of modification of the Document of Security LOPD.
- Present the reports corresponding to:
  - Security audits performed.
  - Verification of compliance with the provisions of the LOPD Security Document.
  - Incidents of a serious nature occurring hat affect the security of Personal Data.
  - Present any other proposal of measures and actions regarding the security of Personal Data.

9.4.3.3 Safety measures and procedures to be implemented in the implementation of RD 1720/2007

In order to comply with the provisions of Title VIII, the following security measures of the personal data processed will be collected:

9.4.3.3.1 Measures to control access to CORPME´s facilities

As described in the corresponding section, CORPME has security controls and measures to restrict the access of outsiders to CORPME units. In addition to the preventive measures, CORPME will keep a registry of access to data processing equipment rooms that support the activity of Trust Service Provider.

Within the security measures and access control, a policy of control of keys and Identification Cards will be defined, with custody of keys not expressly assigned, and authorization for the copying and deposit of the same to the Security Officer. The policy will also establish the security requirements applicable to the identification and custody of keys.

9.4.3.3.2 Control measures of access to information: Permit Policy

CORPME will draw up an inventory of posts with their corresponding levels of authorization for the access, treatment of DP. Access authorizations will be linked in addition to specific users, to certain data processing equipment, whose location, and default configuration will be oriented to ensure the confidentiality and protection of the DP.

The authorization of access to the data contained in a file corresponds to the Responsible of the File.

File Managers or the people, to whom they delegate, are the only ones with competence to grant, alter or cancel the authorized accesses to the systems.

The Security Officer, in collaboration with File Managers and Operative Officers, will establish for each computer system a segmentation of accesses by defining user profiles, specifying the access options allowed and the type of access required (update Or consultation).

Each user will be assigned a profile for each system to which he has access, so that he has only authorized access to the resources that he needs to perform his function.

Each user with access to the systems of the PKI will have a cryptographic key chain with a certificate with the credentials to access the systems allowed with the corresponding permissions.

Each authorized access to SS.II. Must be uniquely identified with the corresponding user.

The generation of user registrations and downloads, as well as the modification of users' access rights, will be processed exclusively through the established means and following the user administration procedure.

In any case, there will be an updated registry of users with authorized access for each information system, to which the Security Officer will have access in their verification and control tasks.

The registration of users of each system shall include at least the following information:

- User name.
- Position and job position held at CORPME.
- User profile.

9.4.3.3.3 Authorized accesses and Password Policy

- All users with access to an information system will have a single access authorization composed of user ID and password.
- In SS.II. A mechanism must be enabled that requires, at least every 60 days, the change of the password for each access authorization.
- The length of the passwords shall be equal to or greater than eight (8) characters. The information system, if allowed, will force the use of this minimum password length.
- Passwords will consist of a combination of alphabetic and numeric characters and will not refer to any recognizable concept, object or idea. Therefore, you should avoid using significant dates, days of the week, months of the year, names of people, telephones, etc. in passwords.

- The system will be disabled for users who attempt to connect consecutively using incorrect identifiers and / or passwords. The maximum number of attempts allowed is three (3).
- When a user has a period of inactivity in the access to an information system greater than seventy-five (75) days, whenever technologically possible, the corresponding account will be blocked.
- The system will store passwords with encryption algorithms, in order to guarantee the confidentiality and integrity of the passwords.

9.4.3.3.4 Logging Access Information

The SS.II. That handle high level DP will automatically maintain a log file (LOG) whose contents will be kept for at least two years and in which at least the following information will be recorded:

- Login user ID.
- Date and time of access.
- File accessed.
- Type of access.
- Access authorized or denied.
- Key or other information that identifies the records accessed by the user.

The mechanisms that allow the registration of the data are the direct responsibility of the Security Officer, without any need to be allowed to deactivate them.

9.4.3.3.5 Security measures for the management of physical data storage media

Access to media containing DP must be restricted and only available to authorized users. Storage must be carried out in adequate premises in terms of environmental control measures and physical access control. The maintenance of the supports must be carried out in a systematic way, in accordance with a policy of identification and inventory carried out by one or more specialized employees who will be responsible for the management of media.

9.4.3.3.6 Security measures applicable to Computer Systems and Communication Networks

The Security Officer shall be the only authorized to define the procedures for assigning access permits and access to data systems and networks that allow access to the DP, in accordance with the criticality levels of the data in question, And of CORPME's own organizational structure.

The use of systems and the access through a data network to the DP should be conditioned to the legitimate possession and correct introduction of the access data (username and password) assigned to the CORPME employee due to the function that And in accordance with this certification practice statement.

Failed fraudulent access attempts, which in any case are limited to a small number of attempts to avoid brute force attacks, will be searched in order to be investigated and prosecuted, keeping the date, time, code And erroneous keys that have been introduced, as well as any other information that allows to identify the responsible of the access failed.

9.4.3.3.7 Structure Personal Data Files

The files containing personal data will be communicated and registered in a timely manner in Spanish Data Protection Agency File Register. The structure of the same as well as the level of the data they contain will be those defined in the communication and initial registration, corresponding to the approval of any modification, and its communication to the Spanish Data Protection Agency to the Security Officer.

9.4.3.3.8 Incident Management

An incident record of the Service will be enabled under the supervision of the Security Officer, where all the incidents that arise during the provision of the Service will be noted. In this registry, the notification of the incident to the corresponding department will be also noted, in order to inquire about it, and the result of the steps taken to resolve it will be recorded.

The lack of communication by the employee who was aware of an incident in the service, the corresponding department, will constitute a disciplinary punishable offense.

The record of incidents must include at least the following information: Date and time of incident occurrence, detailed description of the same, identity of the person who notifies the incident and who is taking care of it; estimated severity of the incident; and response offered, once assigned.

As a method of detection and notification of incidents, the CORPME TSP has security alarms to report abnormal activities in the systems.

The time taken to report any high-impact security incident to interested parties is defined within 24 hours of detection.

Critical vulnerabilities are corrected within 48 hours of their identification.

9.4.3.3.9 Data backup and recovery procedures

In addition to ensuring the confidentiality of personal data, it is also necessary to provide the necessary measures and controls to ensure the integrity and availability of such data for the purposes they serve. Concurrently with the above will be articulated corrective type backup procedures that allow the recovery of the data in case of accidental or malicious deletion, corruption of the files or any cause that makes it impossible to have legitimate access to them.

The definition of the operational procedures for the making of backup copies will be in charge of the Responsible of Security. Likewise, the Security Officer will be responsible, in the case of loss of files, to manage the recovery of the media with the backup data and its restoration in the repositories in production from the information backed up immediately prior to the loss of the files.

9.4.3.3.10 Test Policy with Actual Data

In general, system and application testing will not be performed with actual data. Not with standing the foregoing when it is essential to have such data for the verification of the correct functioning of a system or application, the Safety Officer, with the authorization of the Safety Committee, will arrange for such tests to be performed with due guarantees for the indemnity And data integrity.

9.5 Intellectual Property Rights

In accordance with the Intellectual Property Law approved by RDL 1/1996, of April 12, all rights in intellectual and industrial property related to the systems, documents, patentable procedures, revocation lists and any others related to its Activity as a provider of certification services, will correspond exclusively to CORPME.

The documents and other elements of the TSP of CORPME will be referenced under the hierarchy of OID 17276 assigned by IANA to CORPME.

9.6 Representation and Warranties

9.6.1 CA's Obligations

In particular, the obligations of the Certification Services Provider are as follows:

OCA.1. Perform your operations in accordance with this CPS and CP's application.

OCA.2. Protect your private keys.

OCA.3. Issue certificates in accordance with the CP's applicable to them.

OCA.4. Upon receipt of a valid certificate request, issue certificates conforming to the X.509 v3 standard and the requirements of the application.

OCA.5. Issue certificates that are consistent with the information known at the time of issuance, and free of data entry errors.

OCA.6. Do not publish the user certificates unless established by the corresponding CP.

OCA.7. Revoke the certificates in the terms described in this CPS and in the CP's, publish the revoked certificates in the CRL in the service directory, and Web service, as often as stipulated.

OCA.8. Publish this CPS and the applicable CP's on the website referred to in this document.

OCA.9. Communicate the changes of this CPS and the CP's.

OCA.10. Keeping the Licenses for Use of the certificates, in paper form or electronically, with the applicants for certificates in which they are aware of their obligations and rights, consent to the processing of their personal data by the CA and confirm that the Information provided is correct.

OCA.11. Ensure availability of CRLs.

OCA.12. In the event that the CA proceeds to the revocation of a certificate, notify the users of certificates in accordance with the provisions of this CPS and CP's that apply to them.

OCA.13. Collaborate with audits led by CORPME TSP to validate the renewal of the keys themselves.

OCA.14. Operate in accordance with applicable law. Specifically with:

OCA.14.1. Directive 1999/93 / EC of the European Parliament and of the Council of 13 December 1999 establishing a Community framework for electronic signatures.

OCA.14.2. Law 59/2003, of December 20, on Electronic Signature.

OCA.14.3. The L.O. 15/1999, of 13 December, on the Protection of Personal Data.

OCA.15. Protect, if any, the keys in your custody.

OCA.16. Do not store in any case the data of creation of signature, private key, of the holders of certificates issued for the purpose of being used for Electronic Usage (key Usage = non repudiation).

OCA.17. In the case of cessation of activity, it must notify the holders of the certificates issued by them at least two months in advance.

OCA.18. Keep all information and documentation related to the certificates registered for fifteen (15) years from the date of issue.

9.6.2 RA's Obligations

In particular, they are obligations of the Processing Units:

ORA.1. Provide applicants with the appropriate computer devices so that they can generate with the greatest guarantees a pair of asymmetric keys.

ORA.2. To verify the identity of the holder and the other circumstances of this one demanded in the CP's, establishing because of them the content of the certificate.

ORA.3. Authorize or deny requests for issuance and revocation of certificates.

ORA.4. Immediately notify the Technical Unit of the revocation of any certificate.

ORA.5. Formalize the licenses for the use of the certificates with the holder, filing them together with the documentation indicated in the CP's, for a period of fifteen (15) years from the date of expiration or revocation of the certificate.

ORA.6. To certify, when requested by CORPME or another person with a legitimate interest, that the applicant has been properly identified and that the information on it appears on the certificate corresponds to the data processed in the Unit.

ORA.7. Apply the physical, logical, procedural and personal security controls established in the Security Plan.

ORA.8. Safely store and for a reasonable period the documentation provided in the certificate issuance process and in the suspension / revocation process.

Carry out any other functions that correspond to you, through the personnel that is necessary in each case, as established in this CPS.

9.6.3 License holders obligation

In particular, the following are the obligations of the Subscriber:

OS.1. Provide the Processing Units with accurate, complete and truthful information regarding the data requested by them to carry out the registration process.

OS.2. Inform the managers of PKI of CORPME of any modification of this information.

OS.3. Know, accept and sign the license to use the certificate.

OS.4. Use the certificate for the purposes for which it was issued, in accordance with the applicable CP's .

OS.5. Carefully guard the signature creation device and the password that protects the access to the electronic signature's private key.

OS.6. Inform CORPME as soon as possible, and for any of the channels authorized for this purpose, the existence of any cause of revocation of the certificate.

OS.7. Refrain from using the private key of the certificate from the same moment in which the CA or the RA is requested or suspension warned or revocation of the same, or once the term of validity of the certificate has expired.

OS.8. Destroy the certificate when required by the CA, by virtue of the right of ownership that in any case conserves on the Certificate and when the Certificate expires or is revoked.

OS.9. Do not monitor, manipulate or perform "reverse engineering" acts on the technical implementation (hardware and software) of the certification services, without prior written permission from the CA.

OS.10. Do not transfer or delegate your responsibilities on a certificate that has been assigned to a third party.

OS.11. Install the certificate only on servers that are accessible to the subjectAltName (s) listed in the certificate profile.

OS.12. Respond to CA instructions regarding certificate compromise or certificate misuse within a specified period.

OS.13. Recognize and accept that the CA has the right to immediately revoke if the applicant violates the terms of use or if it finds that the certificate is being used in criminal activities, such as fraud or distribution of malware.

Any other that derives from the law, this CPS or the CP's.

9.6.4 Obligations of third parties who trust or accept certificates

In particular, the obligations of the Third Party are as follows:

OTC.1. Verify, before depositing your trust in a certificate, that it is current and has not been revoked. To this end, you must check the validity and validity of the signing certificate by any of the means available: check the CRL's or Certificate Status Online Query using OCSP, before accepting any digitally signed communication or document with one of the certificates issued by CORPME.

OTC.2. Limit the reliability of the certificates to the permitted uses of the certificates, in accordance with the extensions of the certificates and the corresponding CP.

OTC.3. Assume its responsibility in the correct verification of electronic signatures.

OTC.4. Assume your responsibility in checking the validity, revocation or suspension of the certificates you trust.

OTC.5. Know the guarantees and responsibilities derived from the acceptance of the certificates in which you trust and assume your obligations.

To notify any fact or anomalous situation related to the certificate and that can be considered as cause of revocation of the same.

9.6.5 TSA Obligations

In particular, TSA obligations are as follows:

OTSA.1. To operate in accordance with this CPS and to the internal policies and procedures that are applicable.

OTSA.2. Conduct internal and external reviews to ensure compliance with implementing legislation and internal policies and procedures.

OTSA.3. Provide uninterrupted access to time-stamping services except in case of scheduled outages, temporary synchronization losses or force majeure.

9.6.6 VA Obligations

In particular, the following are obligations of the VA:

OVA.1. To operate in accordance with this CPS and to the internal policies and procedures that are applicable.

OVA.2. Conduct internal and external reviews to ensure compliance with implementing legislation and internal policies and procedures.

OVA.3. Provide uninterrupted access to on-line certificate validation services, except in case of scheduled outages, temporary synchronization losses or force majeure.

9.6.7 Other participant obligations

In particular, the following are obligations of other participants:

The Repository Service must keep the information of the certificates that have been revoked in CRL format accessible to the Holders and Accepting Third Parties.

9.7 Disclaimer

CORPME will be responsible for the use of the certificates issued under the terms of this CPS, the policies applicable to each class of certificate, as well as Law 59/2003 of Electronic Signature, Law 24/2001, and The Instructions issued in matter of electronic Signature by the General Directorate of Registers and Notaries and other norms that develop it.

The responsibility of CORPME shall not extend to the vulnerabilities inherent to the cryptographic algorithms used in the signature system, defined as reference standards by the competent bodies. Notwithstanding the foregoing, CORPME will diligently ensure that its systems are always adapted to the state of the art.

CORPME will not be responsible for damages suffered by the subscriber or a third party, because of the use of their certificates, outside the cases of use expressly admitted. No liability can be claimed for damages to CORPME, if it can prove that its activity as a Certification Services Provider has been developed in full compliance with Law 59/2003 and other applicable laws, this CPS and CP's associated with each kind of certificate. In no case shall

CORPME respond to subscribers' use of certificates, or errors of fact or interpretation that may be committed by those who validate a signature.

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.

CORPME will not be responsible in any case in the following circumstances:

- When circumstances considered of force majeure, such as natural catastrophes, Wars, and other calamities occur that cause a prolonged interruption of the services and supplies necessary for the provision of the service.
- The damages, direct or indirect, caused by the use of certificates and certified keys for uses not permitted or outside their validity period, as well as for the loss or disclosure of the subscriber's private key.
- When the use of the certificates is carried out outside the allowed cases, or if they are revoked or suspended certificates and the interested party does not verify the status of the certificate before granting it their trust.
- Commitment of the private key, by voluntary disclosure of the subscriber or malicious intervention of a third party, and loss or subtraction of the support with the signature creation data.
- For the improper, erroneous or fraudulent use of certificates or lists of Revoked Certificates (CRLs), issued by CORPME.
- For the irrevocable loss of information due to the use of a CORPME digital, certificate for Confidentiality Encryption.
- In case of falsified or fraudulent documentation by the applicant for the certificate.
- Damage caused by misuse of the information contained in the certificate.
- The CA will not be responsible for the content of those documents signed electronically or any other information that is authenticated by a certificate issued by it.
- Failures or errors due to the computer equipment, browsers or applications used by the owner or by the third users of the certificates.
- The direct or indirect damages or damages that are a consequence of the procedures or products used to generate the pair of asymmetric keys to certify when it is the applicant who provides the keys.
- The contents of the documents signed with a digital signature based on a certificate issued by it, or the information contained on a server by the certificate

CORPME will be liable for damage caused to the Subscriber or to the third party in good faith that places its trust in CORPME certificates, when it is intentional or guilty of the provider. The applicable liability regime will be that defined in Law 59/2003, Electronic Signature and in the rest of the applicable legislation.

Notwithstanding the above, the scope of responsibility assumed by CORPME is delimited to the following extremes:

- Guarantee the exact correspondence between the information contained in the certificates and the information provided by the subscriber at the time of issuance.
- Give the subscriber a certificate of the same kind as the requested one.
- Make available to the subscriber in the corresponding QSCD the private key corresponding to the public key identified in the delivered certificate, guaranteeing the full complementarity of both keys.
- Maintain revoked certificate lists and OCSP validation service, permanently updated and accessible.

Other assumptions provided in the current legislation according to which the Certification Services Provider is responsible for the damages caused.

9.8 Limitations of Responsibilities

9.8.1 RA's Responsibilities

The Processing Units authorized by CORPME are responsible for verifying that the data of the requested certificate are correct according to the documentation submitted by the applicant, in any case being responsible for the Trust Service Provider, in accordance with Article 13.5 of the Electronic Signature Law. This verification refers to both personal data and public office or membership of a professional group, by means of the corresponding certificate or official document. Likewise, the Processing Units will be responsible for the filing of all documentation related to the certificates and their applications, and must be filed for a minimum of fifteen (15) years.

The Processing Units are not liable when the non-compliance is due to a fortuitous event or force majeure or if it is beyond their control, such as natural or other disasters, power outages or malfunction of communications systems, Provided that standard safety measures are available. Nor are they liable when the damages are due to subscribers failure or third parties to fulfil any of their obligations, in particular by not verifying the updated CRLs or if certificate subscriber exceeds the limit of the same in terms of its Possible use or the amount of the value of the transactions that can be carried out with them.

9.8.2 TSA Responsibilities

The TSA will not assume any responsibility regarding the use of the time stamps issued for any activity not specified in this CPS and in the CP's.

TSA is not responsible for the content of the data to which the time stamp that it issues and does not respond of possible damages in transactions to which it has applied applies.

TSA does not represent in any way the users or third parties accepting the certificates that it issues.

9.8.3 Loss Limitations

Except as provided in the provisions of this CPS, CORPME's TSP does not assume any other commitment or provide any other guarantee, nor does it assume any other responsibility to holders of certificates or third parties accepting.

9.9 Indemnification

9.9.1 Indemnification for damage caused by CORPME PKI

CORPME will pay the corresponding damages for damages to third parties based on the terms established in Law 59/2003 of December 20, Electronic Signature, its regulations and this CPS. The TSP of CORPME to holders of certificates or third parties who trust or accept the certificates will assume no other responsibility.

9.9.2 Indemnification for damages caused by Subscribers

Subscribers and third parties are responsible for collecting, destroying, tampering with, modifying, tampering with the data of an electronic signature or certificate during or after the date of creation of the certificate and are subject to indemnification pursuant to Law 59/2003 of December 20, Electronic Signature.

9.9.3 Indemnification for Third Party Relief Damages

Subscribers and third parties are responsible for collecting, destroying, tampering with, modifying, tampering with the data of an electronic signature or certificate during or after the date of creation of the certificate and are subject to indemnification pursuant to Law 59/2003 of December 20, Electronic Signature.

9.10 Validity Period

9.10.1 Time Limit

This CPS 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 CPS Replacement and repeal

This CPS 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 CPS 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 CPS, 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

The channels of communication before any notification, demand, request or any other communication required under the practices described in this CPS are:

- E-mail (Produce its effects once the recipient to whom they are addressed has received the communication).
- Registered mail (Directed to the address contained in section 1.10 of this document).
- Contact telephone number listed in section 1.10 of this document.

9.12 Specifications Changes Procedures

9.12.1 Changes Procedures

The Authority with powers to make and approve changes on the CPS and CP's of the TSP of CORPME is the Policy Approval Authority (PSA). The contact details of the AAP can be found in section 1.7 of this document.

9.12.2 Circumstances in which OID must be changed

If changes to the specifications, in the opinion of the AAP, do not affect the acceptability of the certificates, the smaller version number of the document will be increased and the last number of the Object Identifier (OID) that represents it, Greater number of the version of the document, as well as the rest of its associated OID. It is not considered necessary to communicate this type of modifications to the users of the certificates corresponding to the modified CP or CPS.

In the event that the APA deems that changes to the specification may affect the acceptability of the certificates for specific purposes, the larger version number of the document will be increased and the smaller number of the document will be reset to zero. Finally, the last two numbers of the Object Identifier (OID) that represents it will also be modified. For this type of modifications, the users of the corresponding certificates of the modified CP or CPS will be communicated.

9.13 Claims

The party in dispute to CORPME must communicate all claims between users and CORPME, in order to try to resolve it between the same parties.

For the resolution of any conflict that may arise in relation to this CPS or the CP's published, the parties, with waiver of any other jurisdiction that may correspond, are submitted to the Spanish Courts and Tribunals, regardless of where they were Used certificates issued.

9.14 Applicable regulations

The operations and CORPME TSP operation, as well as the present CPS and the CP's that are applicable to each type of certificate, will be subject to the regulations that are applicable to them, and especially to:

- Directive 1999/93 / EC of the European Parliament and of the Council of 13 December 1999 establishing a Community framework for electronic signatures.
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trustworthy services for electronic transactions in the internal market and repealing Directive 1999/93 / EC.
- Law 59/2003, of December 20, on Electronic Signature.
- Organic Law 15/1999, of December 13, on the Protection of Personal Data.
- Royal Decree 1720/2007 of 21 December, which regulates the security measures of automated files containing personal data.
- Law 11/2007, of 22 June, on electronic access of citizens to public services.

9.14.1 Compliance with applicable regulations

The Policy Approval Authority has the responsibility to ensure compliance with the applicable legislation contained in the previous section.

9.15 Various Stipulations

9.15.1 Full Acceptance Clause

All Third Parties that Trust fully assume the content of the latest version of this CPS and applicable CP's.

9.15.2 Independence

In the event that any of the sections contained in this CPS is declared, partially or totally, void or illegal, it will not affect this circumstance to the rest of the document.

9.15.3 Judicial resolution

The disputing party to CORPME shall communicate all claims between users and CORPME, in order to attempt to resolve it between the same parties.

For the resolution of any conflict that may arise in relation to this, CPS or CP's , the parties, with waiver of any other jurisdiction that may correspond, are submitted to the Spanish Courts and Tribunals, regardless of where they were used the certificates issued.

9.16 Other Stipulations

Not stipulated.

10 ANNEXES

10.1 CORPME Certification Practice Statement

This document is a summary of the rights and obligations contained in the **Certification Practice Statement** of **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).** This extract is non-exhaustive and does not exempt the end user from the obligation to consult the complete Declaration in order to be properly informed of their obligations as holder of a digital certificate and their rights to CORPME.

The CPS and the particular CP's applicable to each type of certificate, regulate all aspects related to the life cycle of the certificates, in particular those referring to the application, issuance, acceptance, renewal, reissue and revocation of the same.

The legal relationships between the issuer of the certificates, the users of the certificates and the third parties who rely on the CORPME certificates, will be developed within the framework defined by the CPS and the particular policies that are applicable to each class of certificate.

CORPME issues different types of certificates, both to individuals (as individuals, in the exercise of a profession, position or representation) as legal persons in the cases in which it corresponds. It will be the responsibility of the applicant for a certificate from CORPME to consult the applicable conditions of use, to provide documentation justifying the attributes to certify. The use of the Electronic Signature certificate for purposes not included in its CP's will be done under the full responsibility of the subscriber.

It is subscriber's responsibility to exercise diligent custody of QSCD and the password that protects access to his private key. In case of compromise of this key, or any other assumption, loss or subtraction of the device, which entails a risk of illegitimate use of the Subscriber's Electronic Signature, the subscriber must immediately notify CORPME to proceed with the Revocation of the certificate.

Any change in the data provided to CORPME at the time of requesting the certificate, or the modification or termination of the certified position or representation, must be immediately communicated to CORPME in order to revoke the certificate and, if applicable, issue a new one, which faithfully reflects the new circumstances of the subscriber.

The Certification Practice Statement in its latest version, as well as the other documents related to the provision of the service will be accessible at the URL **http://pki.registradores.org/normativa/index.htm.**

For any query related to the service can be directed to the address contained in the following URL: **http://pki.registradores.org/normativa/direccion.html.**