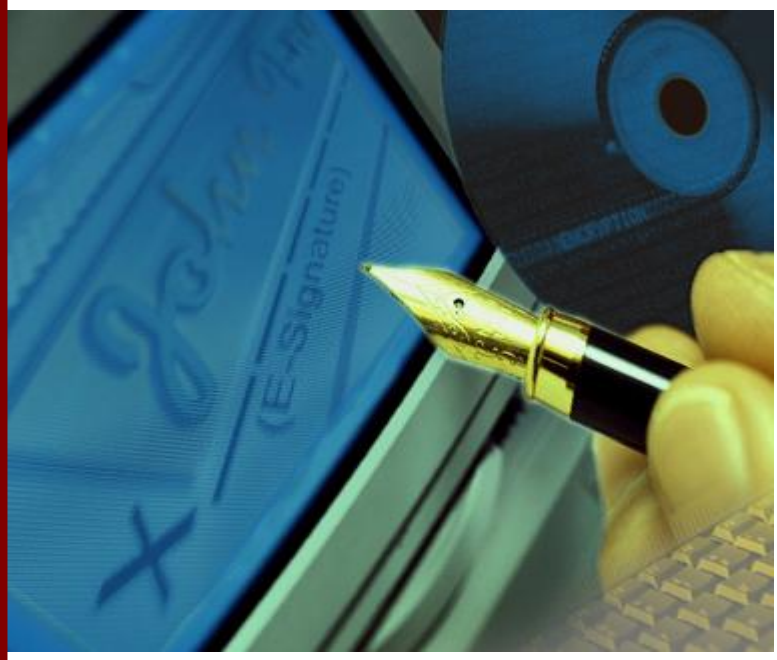
COLEGIO DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

SCR Servicio de Certificación de los Registradores



Política de Certificación de Certificados Externos de Pruebas

Versión 1.0
27 de Enero de 2014

CONTROL DOCUMENTAL

DOCUMENTO/ARCHIVO	
Título: **Política de Certificación de Certificados Externos de Pruebas**	Nombre Archivo/s:
Código:	Soporte lógico:
Fecha: **27/01/2014**	Ubicación física:
Versión: **Versión 1.0**	

REGISTRO DE CAMBIOS		
Versión	Fecha	Motivo del cambio
1.0	27/01/2014	Versión inicial

DISTRIBUCIÓN DEL DOCUMENTO	
Nombre	Área

CONTROL DEL DOCUMENTO			
PREPARADO	**REVISADO**	**APROBADO**	**ACEPTADO**

Índice

1. CLÁUSULAS GENERALES

Los siguientes apartados son comunes a los diferentes certificados recogidos a lo largo del presente documento.

1.1. USO DE LOS CERTIFICADOS

1.1.1. Usos apropiados de los certificados

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

1.1.2. Limitaciones y restricciones en el uso de los certificados

Cualquier uso no incluido en el apartado anterior queda excluido.

1.2. ADMINISTRACIÓN DE LAS PC'S

1.2.1. Entidad Responsable.

El Servicio de Certificación del Colegio de Registradores (en adelante SCR) a través de su Comisión Directora, establecerá los términos y redacción de las Prácticas de Certificación de pruebas (en adelante PC's de pruebas) del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España (en adelante CORPME). En aquellos casos en que de conformidad con lo dispuesto en el Reglamento del SCR sea preceptivo, la Comisión Directora actuará por mandato de la Junta de Gobierno del CORPME, o recabará su autorización en aquellas materias cuya competencia esté reservada al máximo órgano de gobierno de los Registradores.

1.2.2. Procedimiento de aprobación y modificación de las diferentes Políticas de Certificación

La aprobación y subsiguientes modificaciones de las siguientes PC's de pruebas, corresponde en exclusiva a la Comisión Directora del SCR, en virtud de las facultades delegadas por la Junta de Gobierno del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España.

1.2.3. Nombre del documento e identificación

Nombre del documento	Políticas de Certificación (PC) de Certificados Externos de Pruebas
Versión del documento	1.0
Estado del documento	Versión
Fecha de emisión	27/01/2014
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.2.0.1.0
Ubicación de la PC	http://test.pki.registradores.org/normativa/index.htm
DPC Relacionada	Declaración de Prácticas de Certificación de Certificados de Pruebas del Servicio de Certificación del CORPME

1.2.4. Datos de Contacto

Para consultas o comentarios relacionados con las diferentes PC's, el interesado deberá dirigirse al CORPME a través de alguno de los siguientes medios:

Colegio de Registradores de la Propiedad, Mercantiles y de Bienes muebles de España
Servicio de Certificación de los Registradores
C/ DIEGO DE LEON, 21
28006-MADRID
Email: scr@registradores.org
Tlf: 902 020 306

2. TIPOS DE CERTIFICADOS

2.1. CERTIFICADO PERSONAL DE PRUEBAS

2.1.1. Política de certificación

El presente documento recoge la PC de pruebas que el CORPME, aplica a los *Certificados Personales de pruebas*. Esta PC de pruebas desarrolla y complementa lo dispuesto en la DPC de pruebas.

Los efectos legales de un certificado de prueba así como los derechos y obligaciones asociados al mismo, se interpretarán en todo caso atendiendo a la DPC de Pruebas y a la PC de pruebas, en la versión obrante en cada momento en la URL especificada en el propio certificado.

Antes de solicitar un certificado de pruebas o de hacer uso del mismo como mecanismo de comprobación de firmas electrónicas, se recomienda leer el presente documento, al objeto de valorar adecuadamente la confianza que ofrece un certificado digital. No se podrá alegar el desconocimiento de la PC de pruebas para eximirse de responsabilidades propias ni para exigirlas a otra parte.

2.1.2. Definición y finalidad

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de uno o varios certificados en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

Los *Certificados Personales de pruebas* se utilizarán exclusivamente con propósitos de prueba de comprobación autorizada para probar la funcionalidad general de los certificados o bien para simular las funciones propias del certificado de prueba

No se utilizarán para ningún otro propósito, incluidas transacciones comerciales, autenticación de la entidad de un suscriptor o la autoridad de certificación, ni para asegurar la confidencialidad de ninguna información. No se solicitaran ni utilizará un certificado de prueba con ningún propósito que no sea una comprobación técnica autorizada por los suscriptores y los usuarios admiten que ni la identidad ni la autoridad se ha autenticado ni aprobado por la CA de prueba ni por el COPRME

El uso de estos certificados para el cifrado de confidencialidad puede dar lugar a pérdidas irrecuperables de información, ya que el CORPME no dispone de mecanismos de recuperación de claves para esta clase de certificados. Por ello, únicamente se recomienda el cifrado de mensajes para garantizar la confidencialidad durante la transmisión.

En esta PC de prueba se detalla y completa lo estipulado en la DPC de pruebas del CORPME, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

2.1.3. Publicación

El COPRME no asume ninguna responsabilidad en cuanto a la exactitud de la información publicada sobre certificados revocados, ni sobre los mecanismos de actualización de las CRL de prueba.

La lista de *Certificados Personales de pruebas* revocados (CRL) se publica en el Directorio de Validación de Certificados, a efectos de que los usuarios de un certificado puedan comprobar la validez del mismo. El Directorio se publica en la siguiente URL:

- **HTTP**: http://test.pki.registradores.org/crls/test_crl_ext_scr.crl

Esta CRL, firmada por el CORPME, se actualiza cada vez que se revoca un certificado.

Además de la publicación de las CRL's, la PKI dispone de un servicio OCSP de validación de certificados, que implementa la *"RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol"*, en los que se puede consultar el estado de revocación de un determinado certificado emitido por las CA´s de pruebas. La dirección URL de acceso se encuentra publicada en la DPC de pruebas.

El CORPME no ofrece ningún tipo de garantía, ni asumirá responsabilidad alguna sobre la exactitud de la información proporcionada por este servicio.

2.1.4. Contenido

Los certificados están firmados electrónicamente por el CORPME con la clave privada correspondiente a la clase de los certificados externos de prueba y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

La longitud de las claves certificadas es de 1024 bits. El periodo de vigencia es de dos años salvo que se acuerde lo contrario con el suscriptor.

2.1.5. Estructura

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Registro Mercantil Emisor>	Unidad de Tramitación en la que se generó el certificado
CN	TEST - NOMBRE apellidos nombre – NIF nif	Todos estos datos deben ir en MAYÚSCULAS.

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1. 17276.0.2.1.1		
Notice Referente	Certificado de Test de Personal, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2014)		
2. Subject Alternative Names	**Rfc822Name**=correo_personal@domain.com **1.3.6.1.4.1.17276.1.0.0.1**:Dirección Postal	NO	[RFC3280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**1) HTTP:** http://test.pki.registradores.org/crls/test_crl_ext_scr.crl **(2)LDAP:**//test.ldap.registradores.org/CN=TEST%20CA%20EXTERNA,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://test.ocsp.registradores.org **CA Raíz:**http://test.pki.registradores.org/certificados/test_ca_raiz_scr.crt	NO	

2.1.6. Suscriptor del certificado

2.1.6.1. Aceptación del certificado

Según lo especificado en la en la DPC de pruebas del CORPME.

2.1.6.2. Obligaciones del suscriptor

Las obligaciones del suscriptor están recogidas en la DPC de pruebas del CORPME.

2.1.6.3. Responsabilidad del CORPME

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

2.1.7. Requisitos técnicos

Para poder utilizar el *Certificado Personal de prueba*, el suscriptor deberá cumplir con los siguientes requerimientos mínimos de equipos y programas informáticos:

1. Un ordenador personal con acceso a Internet. Se recomienda el uso de un Pentium III 1 GHz o superior, con 128 Mb de RAM, sistema operativo Windows 2000 o superior, y navegador Internet Explorer 6.0 o superior, o Mozilla Firefox 1.5 o superior. Asimismo se recomienda disponer de al menos un conector USB libre, de fácil acceso por el usuario.

2.1.8. Emisión del certificado

2.1.8.1. Procedimiento

El CORPME emitirá un certificado de prueba para un suscriptor una vez recibida una solicitud debidamente cumplimentada. El COPRME proporcionará al suscriptor y a otros usuarios acceso a los certificados intermedios de pruebas y al certificado raíz de pruebas.

2.1.9. Extinción de los certificados

2.1.9.1. Revocación del certificado

2.1.9.1.1. Causas

Según lo especificado en la DPC de pruebas del CORPME.

2.1.9.1.2. Procedimiento

Según lo especificado en la DPC de pruebas del CORPME.

2.1.9.1.3. Efectos

Según lo especificado en la DPC de pruebas del CORPME.

2.1.9.2. Suspensión

Según lo especificado en la DPC de pruebas del CORPME.

2.1.9.3. Caducidad

Según lo especificado en la DPC de pruebas del CORPME.

2.2. CERTIFICADOS DE REPRESENTANTE DE PERSONA JURÍDICA DE PRUEBAS

2.2.1. Política de Certificación

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de uno o varios certificados en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

Los *Certificados de prueba de representante de persona jurídica* se utilizarán exclusivamente con propósitos de prueba de comprobación autorizada para probar la funcionalidad general de los certificados o bien para simular las funciones propias del certificado de prueba

No se utilizarán para ningún otro propósito, incluidas transacciones comerciales, autenticación de la entidad de un suscriptor o la autoridad de certificación, ni para asegurar la confidencialidad de ninguna información. No se solicitaran ni utilizará un certificado de prueba con ningún propósito que no sea una comprobación técnica autorizada por los suscriptores y los usuarios admiten que ni la identidad ni la autoridad se ha autenticado ni aprobado por la CA de prueba ni por el COPRME

El uso de estos certificados para el cifrado de confidencialidad puede dar lugar a pérdidas irrecuperables de información, ya que el CORPME no dispone de mecanismos de recuperación de claves para esta clase de certificados. Por ello, únicamente se recomienda el cifrado de mensajes para garantizar la confidencialidad durante la transmisión.

En esta PC de prueba se detalla y completa lo estipulado en la DPC de pruebas del CORPME, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

2.2.2. Definición y Finalidad

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de uno o varios certificados en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

Los *Certificados de prueba de representante de persona jurídica* se utilizarán exclusivamente con propósitos de prueba de comprobación autorizada para probar la funcionalidad general de los certificados o bien para simular las funciones propias del certificado de prueba

No se utilizarán para ningún otro propósito, incluidas transacciones comerciales, autenticación de la entidad de un suscriptor o la autoridad de certificación, ni para asegurar la confidencialidad de ninguna información. No se solicitaran ni utilizará un certificado de prueba con ningún propósito que no sea una comprobación técnica autorizada por los suscriptores y los usuarios admiten que ni la identidad ni la autoridad se ha autenticado ni aprobado por la CA de prueba ni por el COPRME

El uso de estos certificados para el cifrado de confidencialidad puede dar lugar a pérdidas irrecuperables de información, ya que el CORPME no dispone de mecanismos de recuperación de claves para esta clase de certificados. Por ello, únicamente se recomienda el cifrado de mensajes para garantizar la confidencialidad durante la transmisión.

En esta PC de prueba se detalla y completa lo estipulado en la DPC de pruebas del CORPME, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

2.2.3. Publicación

El COPRME no asume ninguna responsabilidad en cuanto a la exactitud de la información publicada sobre certificados revocados, ni sobre los mecanismos de actualización de las CRL de prueba.

La lista de *Certificados de prueba de representante de persona jurídica* revocados (CRL) se publica en el Directorio de Validación de Certificados, a efectos de que los usuarios de un certificado puedan comprobar la validez del mismo. El Directorio se publica en la siguiente URL:

- **HTTP**: http://test.pki.registradores.org/crls/test_crl_ext_scr.crl

Esta CRL, firmada por el CORPME, se actualiza cada vez que se revoca un certificado.

Además de la publicación de las CRL's, la PKI dispone de un servicio OCSP de validación de certificados, que implementa la *"RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol"*, en los que se puede consultar el estado de revocación de un determinado certificado emitido por las CA´s de pruebas. La dirección URL de acceso se encuentra publicada en la DPC de pruebas.

El CORPME no ofrece ningún tipo de garantía, ni asumirá responsabilidad alguna sobre la exactitud de la información proporcionada por este servicio.

2.2.4. Contenido

Los certificados están firmados electrónicamente por el CORPME con la clave privada correspondiente a la clase de los certificados externos de prueba y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

La longitud de las claves certificadas es de 1024 bits. El periodo de vigencia es de dos años salvo que se acuerde lo contrario con el suscriptor.

2.2.5. Estructura

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Registro Mercantil Emisor>	Unidad de Tramitación en la que se generó el certificado
CN	TEST - ENTIDAD razón social – CIF cif - NOMBRE apellidos nombre – NIF nif	Todos estos datos deben ir en MAYÚSCULAS.

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1. 17276.0.2.2.1		
Notice Referente	Certificado de Representante de prueba, sujeto a la Declaración de Prácticas de Test de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2014)		
2. Subject Alternative Names	**Rfc822Name** = correo_representante@domain.com **1.3.6.1.4.1.17276.1.2.2.3**: Cargo **1.3.6.1.4.1.17276.1.2.2.4**: Datos de Inscripción: Código Flei **1.3.6.1.4.1.17276.1.2.2.5**: Datos de Inscripción: Registro **1.3.6.1.4.1.17276.1.2.2.6**: Datos de Inscripción: Hoja **1.3.6.1.4.1.17276.1.2.2.7**: Datos de Inscripción: Tomo **1.3.6.1.4.1.17276.1.2.2.8**: Datos de Inscripción: Sección **1.3.6.1.4.1.17276.1.2.2.9**: Datos de Inscripción: Libro **1.3.6.1.4.1.17276.1.2.2.10**: Datos de Inscripción: Folio **1.3.6.1.4.1.17276.1.2.2.11**: Datos de Inscripción: Inscripción **1.3.6.1.4.1.17276.1.0.0.1**: Dirección Postal	NO	[RFC3280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**(1) HTTP:** http://test.pki.registradores.org/crls/test_crl_ext_scr.crl **(2)LDAP:**//test.ldap.registradores.org/CN=TEST%20CA%20EXTERNA,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://test.ocsp.registradores.org **CA Raíz:**http://test.pki.registradores.org/certificados/test_ca_raiz_scr.crt	NO	

2.2.6. Suscriptor del certificado

2.2.6.1. Aceptación del certificado

Las obligaciones del suscriptor están recogidas en la DPC de pruebas del CORPME.

2.2.6.2. Obligaciones del suscriptor

Según lo especificado en la DPC de pruebas del CORPME.

2.2.6.3. Responsabilidad del CORPME

Según lo especificado en la DPC de pruebas del CORPME.

2.2.7. Requisitos técnicos

Para poder utilizar el *Certificado de Representante de Persona Jurídica de pruebas*, el suscriptor deberá cumplir con los siguientes requerimientos mínimos de equipos y programas informáticos:

1. Un ordenador personal con acceso a Internet. Se recomienda el uso de un Pentium III 1 GHz o superior, con 128 Mb de RAM, sistema operativo Windows 2000 o superior, y navegador Internet Explorer 6.0 o superior, o Mozilla Firefox 1.5 o superior.

2.2.8. Emisión del certificado

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

2.2.8.1. Procedimiento

El CORPME emitirá un certificado de prueba para un suscriptor una vez recibida una solicitud debidamente cumplimentada. El COPRME proporcionará al suscriptor y a otros usuarios acceso a los certificados intermedios de pruebas y al certificado raíz de pruebas.

2.2.9. Extinción de los certificados

2.2.9.1. Revocación del certificado

2.2.9.1.1. Causas

Según lo especificado en la DPC de pruebas del CORPME.

2.2.9.1.2. Procedimiento

Según lo especificado en la DPC de pruebas del CORPME.

2.2.9.1.3. Efectos

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

2.2.9.2. Suspensión

Según lo especificado en la DPC de pruebas del CORPME.

2.2.9.3. Caducidad

Según lo especificado en la DPC de pruebas del CORPME.

2.3. CERTIFICADOS DE CARGO ADMINISTRATIVO DE PRUEBAS

2.3.1. Política de Certificación

El presente documento recoge la PC de pruebas que el CORPME, aplica a los *Certificados de Cargo Administrativo de pruebas.* Esta PC de pruebas desarrolla y complementa lo dispuesto en la DPC de pruebas.

Los efectos legales de un certificado de prueba así como los derechos y obligaciones asociados al mismo, se interpretarán en todo caso atendiendo a la DPC de Pruebas y a la PC de pruebas, en la versión obrante en cada momento en la URL especificada en el propio certificado.

Antes de solicitar un certificado de pruebas o de hacer uso del mismo como mecanismo de comprobación de firmas electrónicas, se recomienda leer el presente documento, al objeto de valorar adecuadamente la confianza que ofrece un certificado digital. No se podrá alegar el desconocimiento de la PC de pruebas para eximirse de responsabilidades propias ni para exigirlas a otra parte.

2.3.2. Definición y Finalidad

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de uno o varios certificados en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

Los *Certificados de Cargo Administrativo de pruebas* se utilizarán exclusivamente con propósitos de prueba de comprobación autorizada para probar la funcionalidad general de los certificados o bien para simular las funciones propias del certificado de prueba

No se utilizarán para ningún otro propósito, incluidas transacciones comerciales, autenticación de la entidad de un suscriptor o la autoridad de certificación, ni para asegurar la confidencialidad de ninguna información. No se solicitaran ni utilizará un certificado de prueba con ningún propósito que no sea una comprobación técnica autorizada por los suscriptores y los usuarios admiten que ni la identidad ni la autoridad se ha autenticado ni aprobado por la CA de prueba ni por el COPRME

El uso de estos certificados para el cifrado de confidencialidad puede dar lugar a pérdidas irrecuperables de información, ya que el CORPME no dispone de mecanismos de recuperación de claves para esta clase de certificados. Por ello, únicamente se recomienda el cifrado de mensajes para garantizar la confidencialidad durante la transmisión.

En esta PC de prueba se detalla y completa lo estipulado en la DPC de pruebas del CORPME, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

2.3.3. Publicación

El COPRME no asume ninguna responsabilidad en cuanto a la exactitud de la información publicada sobre certificados revocados, ni sobre los mecanismos de actualización de las CRL de prueba.

La lista de *Certificados de Cargo Administrativo de pruebas* revocados (CRL) se publica en el Directorio de Validación de Certificados, a efectos de que los usuarios de un certificado puedan comprobar la validez del mismo. El Directorio se publica en la siguiente URL:

- **HTTP**: http://test.pki.registradores.org/crls/test_crl_ext_scr.crl

Esta CRL, firmada por el CORPME, se actualiza cada vez que se revoca un certificado.

Además de la publicación de las CRL's, la PKI dispone de un servicio OCSP de validación de certificados, que implementa la *"RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol"*, en los que se puede consultar el estado de revocación de un determinado certificado emitido por las CA´s de pruebas. La dirección URL de acceso se encuentra publicada en la DPC de pruebas.

El CORPME no ofrece ningún tipo de garantía, ni asumirá responsabilidad alguna sobre la exactitud de la información proporcionada por este servicio.

2.3.4. Contenido

Los certificados están firmados electrónicamente por el CORPME con la clave privada correspondiente a la clase de los certificados externos de prueba y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

2.3.5. Estructura

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Registro Emisor>	Unidad de Tramitación en la que se generó el certificado
CN	TEST - NOMBRE apellidos nombre – NIF nif	Todos estos datos deben ir en MAYÚSCULAS.

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1. 17276.0.2.3.1		
Notice Referente	Certificado de Cargo Administrativo de pruebas, sujeto a la Declaración de Prácticas de Test de Certificación del		

	Colegio de Registradores de la Propiedad y Mercantiles de España (© 2014)		
2. Subject Alternative Names	**Rfc822Name**=correo_cargo@domain.com **1.3.6.1.4.1.17276.1.2.3.1**: Cargo Administrativo **1.3.6.1.4.1.17276.1.2.3.2**: Administración **1.3.6.1.4.1.17276.1.2.3.3**: Órgano administrativo representado **1.3.6.1.4.1.17276.1.2.3.4**: Unidad local **1.3.6.1.4.1.17276.1.0.0.1**: Dirección Postal	NO	[RFC3280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**(1) HTTP:** http://test.pki.registradores.org/crls/test_crl_ext_scr.crl **(2)LDAP:**//test.ldap.registradores.org/CN=TEST%20CA%20EXTERNA,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://test.ocsp.registradores.org **CA Raíz:**http://test.pki.registradores.org/certificados/test_ca_raiz_scr.crt	NO	

2.3.6. Suscriptor del certificado

2.3.6.1. Aceptación del certificado

Las obligaciones del suscriptor están recogidas en la DPC de pruebas del CORPME.

2.3.6.2. Obligaciones del suscriptor

Según lo especificado en la DPC de pruebas del CORPME.

2.3.6.3. Responsabilidad del CORPME

Según lo especificado en la DPC de pruebas del CORPME.

2.3.7. Requisitos técnicos

Para poder utilizar el *Certificado Reconocido de Cargo Administrativo*, el suscriptor deberá cumplir con los siguientes requerimientos mínimos de equipos y programas informáticos:

1. Un ordenador personal con acceso a Internet. Se recomienda el uso de un Pentium III 1 GHz o superior, con 128 Mb de RAM, sistema operativo Windows 2000 o superior, y navegador Internet Explorer 6.0 o superior, o Mozilla Firefox 1.5 o superior.

2.3.8. Emisión del certificado

2.3.8.1. Procedimiento

El CORPME emitirá un certificado de prueba para un suscriptor una vez recibida una solicitud debidamente cumplimentada. El COPRME proporcionará al suscriptor y a otros usuarios acceso a los certificados intermedios de pruebas y al certificado raíz de pruebas.

2.3.9. Extinción de los certificados

2.3.9.1. Revocación del certificado

2.3.9.1.1. Causas

Según lo especificado en la DPC de pruebas del CORPME.

2.3.9.1.2. Procedimiento

Según lo especificado en la DPC de pruebas del CORPME.

2.3.9.1.3. Efectos

Según lo especificado en la DPC de pruebas del CORPME.

2.3.9.2. Suspensión

Según lo especificado en la DPC de pruebas del CORPME.

2.3.9.3. Caducidad

Según lo especificado en la DPC de pruebas del CORPME.

2.4. CERTIFICADOS DE ADMINISTRACION LOCAL DE PRUEBAS

2.4.1. Política de Certificación

El presente documento recoge la PC de pruebas que el CORPME, aplica a los *Certificados de Administración Local de pruebas.* Esta PC de pruebas desarrolla y complementa lo dispuesto en la DPC de pruebas.

Los efectos legales de un certificado de prueba así como los derechos y obligaciones asociados al mismo, se interpretarán en todo caso atendiendo a la DPC de Pruebas y a la PC de pruebas, en la versión obrante en cada momento en la URL especificada en el propio certificado.

Antes de solicitar un certificado de pruebas o de hacer uso del mismo como mecanismo de comprobación de firmas electrónicas, se recomienda leer el presente documento, al objeto de valorar adecuadamente la confianza que ofrece un certificado digital. No se podrá alegar el desconocimiento de la PC de pruebas para eximirse de responsabilidades propias ni para exigirlas a otra parte.

2.4.2. Definición y Finalidad

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de uno o varios certificados en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

Los *Certificados de Administración Local de pruebas* se utilizarán exclusivamente con propósitos de prueba de comprobación autorizada para probar la funcionalidad general de los certificados o bien para simular las funciones propias del certificado de prueba

No se utilizarán para ningún otro propósito, incluidas transacciones comerciales, autenticación de la entidad de un suscriptor o la autoridad de certificación, ni para asegurar la confidencialidad de ninguna información. No se solicitaran ni utilizará un certificado de prueba con ningún propósito que no sea una comprobación técnica autorizada por los suscriptores y los usuarios admiten que ni la identidad ni la autoridad se ha autenticado ni aprobado por la CA de prueba ni por el COPRME

El uso de estos certificados para el cifrado de confidencialidad puede dar lugar a pérdidas irrecuperables de información, ya que el CORPME no dispone de mecanismos de recuperación de claves para esta clase de certificados. Por ello, únicamente se recomienda el cifrado de mensajes para garantizar la confidencialidad durante la transmisión.

En esta PC de prueba se detalla y completa lo estipulado en la DPC de pruebas del CORPME, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

2.4.3. Publicación

El COPRME no asume ninguna responsabilidad en cuanto a la exactitud de la información publicada sobre certificados revocados, ni sobre los mecanismos de actualización de las CRL de prueba.

La lista de *Certificados de Administración Local de pruebas* revocados (CRL) se publica en el Directorio de Validación de Certificados, a efectos de que los usuarios de un certificado puedan comprobar la validez del mismo. El Directorio se publica en la siguiente URL:

- **HTTP:** http://test.pki.registradores.org/crls/test_crl_ext_scr.crl

Esta CRL, firmada por el CORPME, se actualiza cada vez que se revoca un certificado.

Además de la publicación de las CRL's, la PKI dispone de un servicio OCSP de validación de certificados, que implementa la *"RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol"*, en los que se puede consultar el estado de revocación de un determinado certificado emitido por las CA´s de pruebas. La dirección URL de acceso se encuentra publicada en la DPC de pruebas.

El CORPME no ofrece ningún tipo de garantía, ni asumirá responsabilidad alguna sobre la exactitud de la información proporcionada por este servicio.

2.4.4. Contenido

.Los certificados están firmados electrónicamente por el CORPME con la clave privada correspondiente a la clase de los certificados externos de prueba y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

La longitud de las claves certificadas es de 1024 bits. El periodo de vigencia es de dos años salvo que se acuerde lo contrario con el suscriptor.

2.4.5. Estructura

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Registro Emisor>	Unidad de Tramitación en la que se generó el certificado
CN	TEST - NOMBRE apellidos nombre – NIF nif	Todos estos datos deben ir en MAYÚSCULAS.

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1. 17276.0.2.4.1		
Notice Referente	Certificado de Administración Local de pruebas, sujeto a la Declaración de Prácticas de Test de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2014)		

2. Subject Alternative Names	**Rfc822Name**=correo_cargo@domain.com **1.3.6.1.4.1.17276.1.2.4.1**: Cargo **1.3.6.1.4.1.17276.1.2.4.2**: Provincia de la Administración Local **1.3.6.1.4.1.17276.1.2.4.3**: Unidad local **1.3.6.1.4.1.17276.1.0.0.1**: Dirección Postal	NO	[RFC3280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**(1) HTTP:** http://test.pki.registradores.org/crls/test_crl_ext_scr.crl **(2)LDAP:**//test.ldap.registradores.org/CN=TEST%20CA%20EXTERNA,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://test.ocsp.registradores.org **CA Raíz:**http://test.pki.registradores.org/certificados/test_ca_raiz_scr.crt	NO	

2.4.6. Suscriptor del certificado

2.4.6.1. Aceptación del certificado

Las obligaciones del suscriptor están recogidas en la DPC de pruebas del CORPME.

2.4.6.2. Obligaciones del suscriptor

Según lo especificado en la DPC de pruebas del CORPME.

2.4.6.3. Responsabilidad del CORPME

Según lo especificado en la DPC de pruebas del CORPME.

2.4.7. Requisitos técnicos

Para poder utilizar el *Certificado de Administración Local de prueba*, el suscriptor deberá cumplir con los siguientes requerimientos mínimos de equipos y programas informáticos:

1. Un ordenador personal con acceso a Internet. Se recomienda el uso de un Pentium III 1 GHz o superior, con 128 Mb de RAM, sistema operativo Windows 2000 o superior, y navegador Internet Explorer 6.0 o superior, o Mozilla Firefox 1.5 o superior.

2.4.8. Emisión del certificado

2.4.8.1. Procedimiento

El CORPME emitirá un certificado de prueba para un suscriptor una vez recibida una solicitud debidamente cumplimentada. El COPRME proporcionará al suscriptor y a otros usuarios acceso a los certificados intermedios de pruebas y al certificado raíz de pruebas.

2.4.9. Extinción de los certificados

2.4.9.1. Revocación del certificado

2.4.9.1.1. Causas

Según lo especificado en la DPC de pruebas del CORPME.

2.4.9.1.2. Procedimiento

Según lo especificado en la DPC de pruebas del CORPME.

2.4.9.1.3. Efectos

Según lo especificado en la DPC de pruebas del CORPME.

2.4.9.2. Suspensión

Según lo especificado en la DPC de pruebas del CORPME.

2.4.9.3. Caducidad

Según lo especificado en la DPC de pruebas del CORPME.

2.5. CERTIFICADOS DE PROFESIONAL DE PRUEBAS

2.5.1. Política de Certificación

El presente documento recoge la PC de pruebas que el CORPME, aplica a los *Certificados de Profesional de pruebas.* Esta PC de pruebas desarrolla y complementa lo dispuesto en la DPC de pruebas.

Los efectos legales de un certificado de prueba así como los derechos y obligaciones asociados al mismo, se interpretarán en todo caso atendiendo a la DPC de Pruebas y a la PC de pruebas, en la versión obrante en cada momento en la URL especificada en el propio certificado.

Antes de solicitar un certificado de pruebas o de hacer uso del mismo como mecanismo de comprobación de firmas electrónicas, se recomienda leer el presente documento, al objeto de valorar adecuadamente la confianza que ofrece un certificado digital. No se podrá alegar el desconocimiento de la PC de pruebas para eximirse de responsabilidades propias ni para exigirlas a otra parte.

2.5.2. Definición y Finalidad

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de uno o varios certificados en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

Los *Certificados de Profesional de pruebas* se utilizarán exclusivamente con propósitos de prueba de comprobación autorizada para probar la funcionalidad general de los certificados o bien para simular las funciones propias del certificado de prueba

No se utilizarán para ningún otro propósito, incluidas transacciones comerciales, autenticación de la entidad de un suscriptor o la autoridad de certificación, ni para asegurar la confidencialidad de ninguna información. No se solicitaran ni utilizará un certificado de prueba con ningún propósito que no sea una comprobación técnica autorizada por los suscriptores y los usuarios admiten que ni la identidad ni la autoridad se ha autenticado ni aprobado por la CA de prueba ni por el COPRME

El uso de estos certificados para el cifrado de confidencialidad puede dar lugar a pérdidas irrecuperables de información, ya que el CORPME no dispone de mecanismos de recuperación de claves para esta clase de certificados. Por ello, únicamente se recomienda el cifrado de mensajes para garantizar la confidencialidad durante la transmisión.

En esta PC de prueba se detalla y completa lo estipulado en la DPC de pruebas del CORPME, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

2.5.3. Publicación

El COPRME no asume ninguna responsabilidad en cuanto a la exactitud de la información publicada sobre certificados revocados, ni sobre los mecanismos de actualización de las CRL de prueba.

La lista de *Certificados de Profesional de pruebas* revocados (CRL) se publica en el Directorio de Validación de Certificados, a efectos de que los usuarios de un certificado puedan comprobar la validez del mismo. El Directorio se publica en la siguiente URL:

- **HTTP:** http://test.pki.registradores.org/crls/test_crl_ext_scr.crl

Esta CRL, firmada por el CORPME, se actualiza cada vez que se revoca un certificado.

Además de la publicación de las CRL's, la PKI dispone de un servicio OCSP de validación de certificados, que implementa la *"RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol"*, en los que se puede consultar el estado de revocación de un determinado certificado emitido por las CA´s de pruebas. La dirección URL de acceso se encuentra publicada en la DPC de pruebas.

El CORPME no ofrece ningún tipo de garantía, ni asumirá responsabilidad alguna sobre la exactitud de la información proporcionada por este servicio.

2.5.4. Contenido

Los certificados están firmados electrónicamente por el CORPME con la clave privada correspondiente a la clase de los certificados externos de prueba y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

La longitud de las claves certificadas es de 1024 bits. El periodo de vigencia es de dos años salvo que se acuerde lo contrario con el suscriptor.

2.5.5. Estructura

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Registro Emisor>	Unidad de Tramitación en la que se generó el certificado
CN	TEST - NOMBRE apellidos nombre – NIF nif	Todos estos datos deben ir en MAYÚSCULAS.

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1. 17276.0.2.5.1		
Notice Referente	Certificado de Profesional de prueba, sujeto a la Declaración de Prácticas de Test de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2014)		

2. Subject Alternative Names	**Rfc822Name**=correo_profesional@domain.com **1.3.6.1.4.1.17276.1.2.5.1**: Colectivo profesional al que está adscrito el titular del certificado **1.3.6.1.4.1.17276.1.0.0.1**: Dirección Postal	NO	[RFC3280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**(1) HTTP:** http://test.pki.registradores.org/crls/test_crl_ext_scr.crl **(2)LDAP:**//test.ldap.registradores.org/CN=TEST%20CA%20EXTERNA,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://test.ocsp.registradores.org **CA Raíz:**http://test.pki.registradores.org/certificados/test_ca_raiz_scr.crt	NO	

2.5.6. Suscriptor del certificado

2.5.6.1. Aceptación del certificado

Las obligaciones del suscriptor están recogidas en la DPC de pruebas del CORPME.

2.5.6.2. Obligaciones del suscriptor

Según lo especificado en la DPC de pruebas del CORPME.

2.5.6.3. Responsabilidad del CORPME

Según lo especificado en la DPC de pruebas del CORPME.

2.5.7. Requisitos técnicos

Para poder utilizar el *Certificado de Profesional de pruebas*, el suscriptor deberá cumplir con los siguientes requerimientos mínimos de equipos y programas informáticos:

1. Un ordenador personal con acceso a Internet. Se recomienda el uso de un Pentium III 1 GHz o superior, con 128 Mb de RAM, sistema operativo Windows 2000 o superior, y navegador Internet Explorer 6.0 o superior, o Mozilla Firefox 1.5 o superior.

2.5.8. Emisión del certificado

2.5.8.1. Procedimiento

El CORPME emitirá un certificado de prueba para un suscriptor una vez recibida una solicitud debidamente cumplimentada. El COPRME proporcionará al suscriptor y a otros usuarios acceso a los certificados intermedios de pruebas y al certificado raíz de pruebas.

2.5.9. Extinción de los certificados

2.5.9.1. Revocación del certificado

2.5.9.1.1. Causas

Según lo especificado en la DPC de pruebas del CORPME.

2.5.9.1.2. Procedimiento

Según lo especificado en la DPC de pruebas del CORPME.

2.5.9.1.3. Efectos

Según lo especificado en la DPC de pruebas del CORPME.

2.5.9.2. Suspensión

Según lo especificado en la DPC de pruebas del CORPME.

2.5.9.3. Caducidad

Según lo especificado en la DPC de pruebas del CORPME.