

Autoridad de Certificación de la Abogacía



Referencia: CP2_ACATC_004.0

Fecha: 27/06/2016

Estado del documento: **Publicado**



**Consejo General de la
Abogacía Española**

POLÍTICAS DE CERTIFICACIÓN (CP) DE LA AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

CP2_ACATC_004.0 CERTIFICADOS CUALIFICADOS DE SELLO ELECTRÓNICO (VERSIÓN 004.0)

El presente documento no puede ser reproducido, distribuido, comunicado públicamente, archivado o introducido en un sistema de recuperación de información, o transmitido, en cualquier forma y por cualquier medio (electrónico, mecánico, fotográfico, grabación o cualquier otro), total o parcialmente, sin el previo consentimiento por escrito del Consejo General de la Abogacía Española.

Las solicitudes para la reproducción del documento o la obtención de copias del mismo deben dirigirse a:

Administración ACABOGACÍA
Consejo General de la Abogacía Española
Paseo de Recoletos, 13
28004 Madrid

Control del Cambios

Fecha	Versión	Cambios
01/10/2010	CP2_ACATC_001.0	Versión inicial
01/03/2012	CP2_ACATC_002.0	Se elimina referencia a la LAECSP y a los certificados reconocidos
13/03/2014	CP2_ACATC_003.0	Se incluye una descripción de la Jerarquía PKI Se elimina detalles del modelo de módulo Criptográfico Se incrementa la longitud de las claves de usuario a 2048 bits Se indican los nuevos puntos de distribución de CRL Corrección de erratas
27/06/2016	CP2_ACATC_004.0	Se incluye nueva Jerarquía PKI, información nuevos certificados CAs Se alinea con eIDAS Adaptación de servicios reconocidos a cualificados

Índice de Contenido

1. Introducción	5
1.1. Vista General	5
1.2. Identificación	7
1.3. Comunidad y Ámbito de Aplicación.	8
1.4. Datos de contacto	10
2. Cláusulas Generales	11
2.1. Obligaciones	11
2.2. Responsabilidad	11
2.3. Responsabilidad financiera	12
2.4. Interpretación y ejecución	13
2.5. Tarifas	13
2.6. Publicación y Registro de Certificados	14
2.7. Auditorias	15
2.8. Confidencialidad y Protección de Datos Personales	15
2.9. Derechos de propiedad intelectual	16
3. Identificación y Autenticación	17
3.1. Registro inicial	17
3.2. Renovación de certificados	19
3.3. Reemisión después de una revocación	20
3.4. Solicitud de revocación	20
4. Requerimientos Operacionales	21
4.1. Solicitud de certificados	21
4.2. Emisión de certificados	21
4.3. Aceptación de certificados	21
4.4. Suspensión y Revocación de certificados	22
4.5. Procedimientos de Control de Seguridad	22
5. Controles de Seguridad Física, Procedimental y de Personal	23
6. Controles de Seguridad Técnica	24
6.1. Generación e instalación del par de claves	24
6.2. Protección de la clave privada	25
6.3. Estándares para los módulos criptográficos	25
6.4. Ciclo de vida de los dispositivos criptográficos	25
6.5. Controles de seguridad	26
6.6. Controles de ingeniería de los módulos criptográficos	26
7. Perfiles de Certificado	27
7.1. Perfil de Certificado	27
7.2. Perfil de CRL	32

8.	<i>Especificación de la administración</i>	34
8.1.	Autoridad de las políticas	34
8.2.	Procedimientos de especificación de cambios	34
8.3.	Publicación y copia de la política	34
8.4.	Procedimientos de aprobación de la Política	34
<i>ANEXO 1: Información técnica</i>		35
1.	Dispositivos del suscriptor	35
2.	Creación y verificación de firmas	35
2.1.	Estándares y parámetros admitidos	35
2.2.	Métodos de verificación de firmas	35
2.3.	Verificación de la Firma Electrónica a lo largo del tiempo	36
<i>ANEXO 2: ACRONIMOS</i>		38

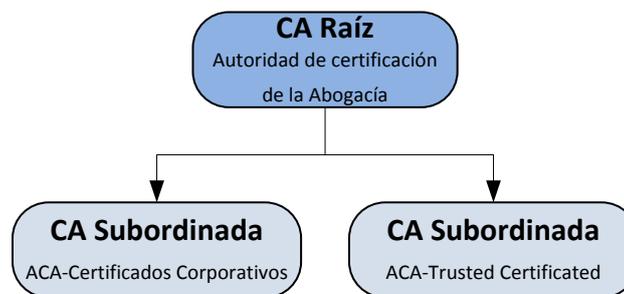
1. Introducción

1.1. Vista General

El Consejo General de la Abogacía Española (CGAE) es el órgano representativo, coordinador y ejecutivo superior de los Ilustres Colegios de Abogados de España y tiene, a todos los efectos, la condición de corporación de derecho público, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines.

El Consejo General de la Abogacía Española se constituye en Prestador de servicios de Certificación mediante la creación de una jerarquía PKI propia. En este sentido, tal como establece la medida transitoria 3 del artículo 51 del Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, un prestador de servicios de certificación que emita certificados reconocidos conforme a la Directiva 1999/93/CE debe presentar un informe de evaluación de conformidad al organismo supervisor lo antes posible, pero no más tarde del 1 de julio de 2017. Hasta que el prestador de servicios de certificación presente dicho informe de evaluación de conformidad y el organismo supervisor ultime su análisis, el mencionado prestador de servicios de certificación será considerado como prestador cualificado de servicios de confianza.

La estructura general de la PKI de ACA está compuesta de dos niveles

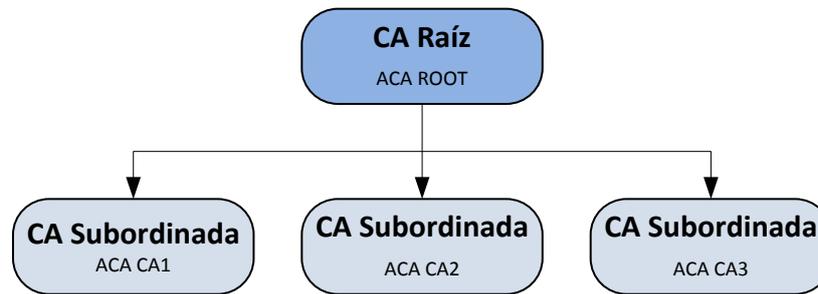


En el año 2014 se han generado nuevas CAs subordinadas con la misma denominación seguida del año de emisión: *ACA – Certificados Corporativos 2014* y *ACA-Trusted Certificates 2014*.

Los certificados emitidos por ambas CAs subordinadas tendrán continuidad con los mismos OID en las CAs versión de 2014.

Por otro lado, en el año 2016 se han generado una nueva CA Raíz y CAs subordinadas en conformidad con la legislación vigente y se mantienen las descritas puesto que se encuentran en vigor los certificados expedidos por estas jerarquías. Se expedirán nuevos certificados mediante las nuevas CAs subordinadas.

Nueva Jerarquía 2016, compuesta de nos niveles;



El presente documento especifica la Política de Certificación del Certificado digital denominado “**Certificado Cualificado de Sello electrónico**” emitido por la autoridad de certificación del Consejo General de la Abogacía Española, o AC Abogacía.

El Consejo General de la Abogacía Española, como entidad reguladora de la abogacía, ha establecido un sistema propio de certificación con el objeto de expedir certificados para diversos usos y diferentes usuarios finales. Por este motivo, se establecen tipos de certificados. Los certificados son expedidos a entidades finales, incluyendo colegiados, personal administrativo y de servicio, organizaciones y personas físicas que representan a dichas organizaciones, por Prestadores de Certificación Acreditados.

Esta Política de Certificación está en conformidad con las disposiciones legales que rigen el asunto de Firma Electrónica en la Comunidad Europea y en España, cumpliendo todos los requisitos técnicos y de seguridad exigidos para emisión de Certificados Reconocidos y está basada en la especificación del estándar RCF 3647 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta estándares europeos, entre los que cabe destacar los siguientes:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
(NOTA: Dicha Directiva será derogada cuando la gran mayoría del articulado de eIDAS sea aplicable, es decir, a partir del 1 de julio de 2016).
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015).
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal, como su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que en su Disposición final sexta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social, que en su disposición final cuarta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de Octubre de 2016).

La Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Abogacía que establece los términos concretos del servicio prestado se puede encontrar en <http://www.acabogacia.org/doc>.

En lo que se refiere al contenido de esta CP, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto.

1.2. Identificación

	CERTIFICADOS CUALIFICADOS DE SELLO ELECTRÓNICO	Políticas de Certificación
---	---	-----------------------------------

Nombre:	CP2_ACATC_004.0
O.I.D.	1.3.6.1.4.1.16533.20.3.1
Descripción:	Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: Certificados cualificados de sello electrónico
Versión:	004.0
Fecha de Emisión:	27/06/2016
Localización:	www.acabogacia.org/doc
CPS relacionada	
O.I.D.	1.3.6.1.4.1.16533.10.1.1
Descripción:	Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Abogacía
Localización:	www.acabogacia.org/doc

1.3. Comunidad y Ámbito de Aplicación.

1.3.1 Autoridad de Certificación (AC)

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Usuario, en las relaciones electrónicas, esta Política permite identificar y vincular un determinado sistema o plataforma a una determinada entidad (Suscriptor) relacionada a un Colegio Profesional concreto a través de la emisión de un Certificado.

La información relativa a la AC puede encontrarse en la dirección web www.acabogacia.org.

1.3.2 Autoridad de Registro (AR)

Ente que actúa conforme esta Política de Certificación y, en su caso, mediante acuerdo suscrito con la AC, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y aquellas que se dispongan en las Prácticas de Certificación concretas.

A los efectos de la presente Política, la AR es el Consejo General de la Abogacía Española (CGAE)

1.3.3 Prestador de servicios de certificación (PSC) / Prestador cualificado de Servicios de Confianza.

Entendemos bajo la presente política a un PSC como aquella entidad que presta servicios concretos relativos al ciclo de vida de los certificados.

Las funciones de PSC pueden ser desempeñadas directamente por la AC o por una entidad delegada.

Por otro lado, tal como establece el apartado 3 de la medida transitoria del artículo 51 del Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, un prestador de servicios de certificación que emita certificados reconocidos conforme a la Directiva 1999/93/CE debe presentar un informe de evaluación de conformidad al organismo supervisor lo antes posible, pero no más tarde del 1 de julio de 2017. Hasta que el prestador de servicios de certificación presente dicho informe de evaluación de conformidad y el organismo supervisor ultime su análisis, el mencionado prestador de servicios de certificación será considerado como prestador cualificado de servicios de confianza.

Por todo lo anterior, AC Abogacía, actúa como prestador cualificado de servicios de confianza, emitiendo certificados cualificados de sello electrónico y proveyendo servicios de firma electrónica basados en certificados cualificados, conforme a lo establecido en el reglamento 910/2014 de la Unión Europea y en la Ley 59/2003 de Firma electrónica.

1.3.4 Suscriptor

Bajo esta Política los suscriptores podrán ser los Colegios de profesionales, los Consejo General de las profesiones y los Consejos Autonómicos poseedor de un “certificado cualificado de sello de electrónico” y, en general, cualquier persona jurídica vinculada o relacionada de alguna forma con las profesiones.

1.3.5 Usuario

En esta Política se entiende por Usuario, tercera parte confiante, la persona que voluntariamente confía en el Certificado, en virtud de la confianza depositada en la AC, lo utiliza como medio de identificación y autenticación de un sistema o aplicación así como medio para autenticar los documentos electrónicos que este produzca. y en consecuencia se sujeta a lo dispuesto en esta Política, en la Declaración de Prácticas de Certificación (CPS)aplicable y la legislación vigente, por lo que no se requerirá acuerdo posterior alguno.

1.3.6 Solicitante

A los efectos de esta política el solicitante es la persona física que solicita el certificado cualificado de sello electrónico.

1.3.7 Ámbito de Aplicación y Usos

El Certificado emitido bajo la presente Política permite identificar y vincular un determinado sistema o plataforma a una determinada entidad, ya sea un Colegio de profesional, un Consejo General de una profesión o un Consejo Autonómico, así como cualquier persona jurídica vinculada al ejercicio profesional de la Abogacía, permitiendo además autenticar los documentos electrónicos que el Sistema produzca.

1.3.8 Límites y prohibiciones de uso de los certificados

Bajo la presente Política no se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Practicas de Certificación.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la AC.

El Suscriptor o el Usuario que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, la AC tenga responsabilidad alguna en el caso de cifrado de información usando las claves asociadas al certificado.

1.4. Datos de contacto

Organización responsable:

**Autoridad de Certificación de la Abogacía.
Consejo General de la Abogacía Española**

Persona de contacto:

Administrador AC Abogacía
Departamento de Operaciones

E-mail: info@acabogacia.org

Teléfono: Tel. 902 41 11 41

Fax 915327836

Dirección: Consejo General de la Abogacía Española
Paseo de Recoletos, 13
28004 Madrid

2. Cláusulas Generales

2.1. Obligaciones

2.1.1 AC

La AC se obliga según lo dispuesto en las Prácticas de Certificación así como lo dispuesto en la normativa sobre prestación de servicios de Certificación, la Ley 59/2003 y eIDAS, donde sean aplicables.

2.1.2 AR

Las Autoridades de Registro son delegadas por la AC para realizar esta labor, por lo tanto la AR también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados.

2.1.3 Solicitante

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.1.4 Suscriptor

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.1.5 Usuario

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.1.6 Registro de Certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.2. Responsabilidad

El Consejo General de la Abogacía Española, en su actividad de Prestador de Servicios de Certificación / *Prestador cualificado de servicios de confianza* responderá de acuerdo con la Ley de Firma Electrónica, eIDAS y el resto de la legislación aplicable.

En esta misma línea, la AC responderá según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.2.1 Exoneración de responsabilidad

La relación entre la AC y las AR se regirá por su especial relación contractual. La AC y la AR se exonerarán de su responsabilidad en los términos establecidos en la Declaración de Prácticas de Certificación (CPS) y las políticas de certificación. En particular, la AC y la AR no serán responsables en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

1. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Declaración de Prácticas de Certificación (CPS), en particular por la utilización de un certificado suspendido o revocado, o por depositar la confianza en él sin verificar previamente el estado del mismo.
2. Por el uso indebido o fraudulento de los certificados o CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.
3. Por el uso indebido de la información contenida en el Certificado o en la CRL.
4. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Usuarios en la normativa vigente, la Declaración de Prácticas de Certificación (CPS) o en la Política de Certificación correspondiente.
5. Por el contenido de los mensajes o documentos firmados.
6. Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.
7. Fraude en la documentación presentada por el solicitante.

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

La AC limita su responsabilidad según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.3. Responsabilidad financiera

La AC, en su actividad como prestador cualificado de servicios de confianza mantiene recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad de Prestador tal como se establece la legislación aplicable.

En concreto la garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a 3.000.000 €.

2.4. Interpretación y ejecución

2.4.1 Legislación

La ejecución, interpretación, modificación o validez de la presente Política se regirá por lo dispuesto en la legislación española vigente.

2.4.2 Independencia

La invalidez de una de las cláusulas contenidas en esta Política no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

2.4.3 Notificación

Cualquier notificación referente a la presente Política se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

2.4.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

2.5. Tarifas

2.5.1 Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los usuarios en las diferentes Autoridades de Registro.

2.5.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos será gratuito, no obstante, la AC podrá imponer alguna tarifa para los casos de descarga masiva de certificados o cualquier otra circunstancia que a juicio de la AC deba ser gravada, en cuyo caso se publicarán dichas tarifas en la página web de la AC.

2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

La AC proveerá de un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito, por medio de la publicación de la CRL. No obstante, la AC podrá imponer alguna tarifa para otros medios de comprobación del estado de los

certificados o cualquier otra circunstancia que a juicio de la AC deba ser gravada, en cuyo caso se publicarán dichas tarifas en la página web de la AC.

2.5.4 Tarifas por otros servicios

Las tarifas aplicables a otros servicios se publicarán en la página web de la AC.

2.5.5 Política de reintegros

Sin estipulación.

2.6. Publicación y Registro de Certificados

2.6.1 Publicación de información de la AC

2.6.1.1 Políticas y Prácticas de Certificación

La presente Política de Certificación y sus distintas versiones estarán disponibles públicamente en el sitio de Internet <http://www.acabogacia.org/doc>

2.6.1.2 Términos y condiciones

AC Abogacía pondrá a disposición de los Suscriptores y Usuarios los términos y condiciones del servicio en el sitio de Internet <http://www.acabogacia.org/doc>

2.6.1.3 Difusión de los certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.6.2 Frecuencia de publicación

AC Abogacía publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación, manteniendo un histórico de versiones.

AC Abogacía publicará los certificados en el Registro de Certificados inmediatamente después de haber sido emitidos.

Ordinariamente la AC publicará una lista de certificados revocados de oficio con una periodicidad de 24 horas. AC Abogacía publicará de forma extraordinaria una nueva lista de revocación en el momento en que tramita una petición de suspensión o revocación autenticada.

2.6.3 Controles de acceso

AC Abogacía empleará diversos sistemas para la publicación y distribución de certificados y CRL's. Se necesitará tener unos datos de acceso para realizar consultas múltiples.

En la web de AC Abogacía existirán accesos al directorio para la consulta de CRL y Certificados bajo el control de una aplicación y protegiendo la descarga indiscriminada de información.

Las CRL's podrán descargarse de forma anónima mediante protocolo http.

2.7. Auditorias

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.8. Confidencialidad y Protección de Datos Personales

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

2.8.1 Tipo de información a mantener confidencial

La AC considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

2.8.2 Tipo de información considerada no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente Política y en las Prácticas de Certificación.
- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo de manera no exhaustiva:
- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza.
- El nombre y los apellidos del suscriptor del certificado, en caso de certificados individuales, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico del suscriptor del certificado, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de

colectivo, o la dirección de correo electrónico asignada por el suscriptor, en caso de certificados para dispositivos.

- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.

2.8.3 Divulgación de información de revocación / suspensión de certificados

Se difundirá la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRLs. Los detalles del servicio se registrarán por lo dispuesto en la Declaración de Prácticas de Certificación (CPS).

2.8.4 Envío a la Autoridad Competente

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

2.9. Derechos de propiedad intelectual

La propiedad intelectual de estas Políticas pertenece al CGAE. La AC será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita.

La AC concederá licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta política, y de acuerdo con el correspondiente instrumento vinculante entre el AC Abogacía y la parte que reproduzca y/o distribuya el certificado.

Las anteriores reglas figurarán en los instrumentos vinculantes entre la AC y los suscriptores y los terceros que confían en certificados.

3. Identificación y Autenticación

3.1. Registro inicial

3.1.1 Tipos de nombres

Todos los certificados requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.509, y los atributos especificados en la recomendación ITU-T X.520 [1]

El DN de los certificados cualificados de sello electrónico contendrá los elementos que se citan con el formato siguiente. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

- Un componente Nombre (Common Name) –CN
 - Un componente E-mail –E
 - Un componente Organización –O
 - Un componente Identificador de la Organización –OI
 - Un componente Unidad en la Organización –OU
 - Un componente Estado (Country)-C
 - Un componente Número de Serie –serialNumber
 - Un componente localidad- L
-
- El valor autenticado del componente Nombre (Common Name) –CN contendrá la denominación del sistema o aplicación de proceso automático
 - El valor autenticado del componente E-mail –E contendrá la dirección de correo de contacto de la entidad suscriptora del certificado
 - El valor autenticado del componente Organización –O contendrá el nombre de la organización (suscriptor del certificado)
 - El valor autenticado del componente Identificador de la Organización –OI contendrá una identificación del suscriptor diferente del nombre de la organización (suscriptor del certificado). Este valor cumplirá la semántica definida en el apartado 5, de ETSI EN 319 412-1 [i.4]

- El valor autenticado del componente Unidad en la Organización –OU contendrá la naturaleza del certificado (sello electrónico para la actuación automatizada).
- El valor autenticado del componente Estado (Country)-C contendrá “ES”
- El valor autenticado del componente Número de Serie –serialNumber contendrá el CIF de la entidad.
- El valor autenticado del componente Localidad-L contendrá la ubicación de la sede social de la entidad suscriptora

3.1.2 Pseudónimos

Los certificados cualificados de sello electrónico no admiten pseudónimos.

3.1.3 Reglas utilizadas para interpretar varios formatos de nombres

Se atiende en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

3.1.4 Unicidad de los nombres

Los nombres distinguidos de los certificados emitidos serán únicos para cada suscriptor. La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres de los certificados emitidos. El atributo de la Razón Social de la entidad, y/o el CIF darán para distinguir entre dos identidades cuando exista algún problema sobre duplicidad de nombres.

3.1.5 Procedimiento de resolución de disputas de nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

La AC no tiene responsabilidad en el caso de resolución de disputas de nombres. El Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza no deberá determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

El Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

La asignación de nombres se realizará basándose en su orden de entrada.

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

No se admitirán marcas registradas como datos de identificación del Suscriptor. En todo caso se identificará a través de la Razón Social.

3.1.7 Métodos de prueba de la posesión de la clave privada

EL envío del PKCS10 por el suscriptor constituirá la garantía de que el suscriptor está en posesión de la clave privada.

3.1.8 Autenticación de la identidad de un individuo

Para realizar una correcta verificación de la identidad del solicitante, se exigirá documentación que lo acredite y su personación física ante la AR y la presentación del Documento Nacional de Identidad o Tarjeta de Extranjero ante un operador o personal debidamente autorizado de la Autoridad de Registro y demostración de su vinculación con la persona jurídica.

La AR verificará con sus propias fuentes de información el resto de datos y atributos a incluir en el certificado (nombre distinguido del certificado), debiendo guardar la documentación acreditativa de la validez de aquellos datos que no puede comprobar por medio de sus propias fuentes de datos.

3.1.9 Requerimientos aplicables a las AR's externas

Cuando la AC emplee AR's externas deberá asegurar los siguientes aspectos:

- Que existe un contrato en vigor entre la AC y la AR, concretando los aspectos concretos de la delegación y las responsabilidades de cada agente.
- Que la identidad de la AR y de los operadores de la AR ha sido correctamente comprobada y validada.
- Que los operadores de la AR han recibido formación suficiente para el desempeño de sus funciones.
- Que la AR asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones.
- Que la comunicación entre la AR y la AC, se realiza de forma segura mediante el uso de certificados digitales.
- Que las ARs se comprometen a cumplir con los requerimientos generales de seguridad indicados por la AC.

3.2. Renovación de certificados

La renovación de certificados consistirá en la emisión de un nuevo certificado al suscriptor a la fecha de caducidad del certificado original. Antes de renovar un certificado, la AR

deberá comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor continúan siendo válidos.

Si cualquier información del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información.

3.3. Reemisión después de una revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

3.4. Solicitud de revocación

Pueden solicitar la suspensión o revocación de un certificado:

- El propio suscriptor que deberá identificarse ante la AR para solicitar la revocación de su certificado.
- Los operadores autorizados de la AR.
- Los operadores autorizados de la AC o de la jerarquía de certificación.

En cualquiera de los dos últimos casos deberán concurrir las circunstancias que se establecen en el apartado correspondiente, y se procederá en la forma allí descrita a realizar y tramitar las solicitudes de revocación.

4. Requerimientos Operacionales

4.1. Solicitud de certificados

La AR gestiona las solicitudes de Certificados de sello electrónico

La solicitud de un certificado digital podrá realizarse de la siguiente forma:

- Personándose el solicitante en la Autoridad de registro ante un operador debidamente autorizado

Antes de iniciar el proceso de emisión, la AR informa al solicitante del proceso de emisión, las responsabilidades y las condiciones de uso del certificado y del dispositivo, así como verifica la identidad del solicitante, y los datos a incluir en el certificado.

Si la verificación es correcta se procede a la firma del instrumento jurídico vinculante entre el solicitante y la AC – AR.

4.2. Emisión de certificados

El proceso seguido para la emisión de certificados es el siguiente:

- La AR recibe la petición de emisión del certificado.
- El operador de la AR verifica nuevamente el contenido del mismo y si la verificación es correcta lo valida y tramita la aprobación de la emisión para la AC. Si la petición no es correcta, el operador deniega la petición.
- La AR envía por un canal seguro la petición a la AC para la emisión del correspondiente certificado.
- La AC emite el certificado. El certificado generado es enviado de forma segura al solicitante
- La AC notifica al suscriptor/solicitante la emisión del mismo.
- El certificado generado es enviado de forma segura al Registro de Certificados, que lo pone a disposición de los usuarios

4.3. Aceptación de certificados

A partir de la entrega del certificado, el suscriptor dispondrá de un periodo de siete días naturales para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a la AC y el contenido del certificado, ello deberá ser comunicado de inmediato a la AC para que proceda a su revocación y a la emisión de un nuevo certificado.

La AC entregará el nuevo certificado sin coste para el suscriptor en el caso de que la diferencia entre los datos sea causada por un error no imputable al suscriptor.

Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el suscriptor ha confirmado la aceptación del certificado y de todo su contenido. Aceptando el certificado, el suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

4.4. Suspensión y Revocación de certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

4.5. Procedimientos de Control de Seguridad

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

5. Controles de Seguridad Física, Procedimental y de Personal

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

6. Controles de Seguridad Técnica

6.1. *Generación e instalación del par de claves*

6.1.1 Generación del par de claves del suscriptor

La AC realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves sean generadas de acuerdo a los estándares. El par de claves será generado y custodiado por el propio suscriptor o bajo su control.

6.1.2 Entrega de la clave pública al emisor del certificado

El PKCS10 generado por el suscriptor tiene que ser transferido a la AC, de forma que se asegure que:

- No ha sido modificado durante el envío.
- El remitente está en posesión de la clave privada que corresponde con la clave pública transferida.
- El proveedor de la clave pública es el legítimo usuario que aparece en el certificado.

6.1.3 Entrega de la clave pública de la CA a los Usuarios

El certificado de las CAs de la cadena de certificación y su fingerprint estarán a disposición de los usuarios en <http://www.acabogacia.org/doc>

6.1.4 Tamaño y periodo de validez de las claves

6.1.4.1 Tamaño y periodo de validez de las claves del emisor

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

6.1.4.2 Tamaño y periodo de validez de las claves del suscriptor

Las claves privadas del suscriptor están basadas en el algoritmo RSA con una longitud mínima de 2048 bits.

El periodo de uso de la clave pública y privada del suscriptor puede corresponder con la validez temporal de los certificados, no pudiendo ser en ningún caso superior a 4 años.

6.1.5 Parámetros de generación de la clave pública

No estipulado.

6.1.6 Comprobación de la calidad de los parámetros

No estipulado.

6.1.7 Hardware/software de generación de claves

Las claves de las CA vinculadas son generadas en un módulo criptográfico validado FIPS 140-2 nivel 3.

6.1.8 Fines del uso de la clave

Todos los certificados incluirán la extensión Key Usage y extended Key Usage indicando los usos habilitados de la claves.

6.2. Protección de la clave privada

6.2.1 Clave privada de la AC

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

6.2.2 Clave privada del suscriptor

La clave privada del suscriptor será controlada y gestionada por el Representante. Tiene un sistema de protección contra intentos de acceso.

6.3. Estándares para los módulos criptográficos

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

6.4. Ciclo de vida de los dispositivos criptográficos

6.4.1 Ciclo de vida de los dispositivos cualificados de creación de firma electrónica (DCCFE)

No estipulado

6.5. Controles de seguridad

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

6.6. Controles de ingeniería de los módulos criptográficos

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>

7. Perfiles de Certificado

7.1. Perfil de Certificado

Todos los certificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3, la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile. y la RFC 3739 (que sustituye a RFC 3039) "Qualified Certificates Profile". También se ha tenido en cuenta la familia 319 412 en relación a los perfiles de los certificados.

Los certificados cualificados de sello electrónico incluirán, al menos, los siguientes datos:

- a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de sello electrónico;
- b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y
 - para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
 - para personas físicas, el nombre de la persona;
- c) al menos, el nombre del creador del sello y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;
- d) los datos de validación del sello electrónico que correspondan a los datos de creación del sello electrónico;
- e) los datos relativos al inicio y final del período de validez del certificado;
- f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;
- g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
- h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);
- i) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;
- j) cuando los datos de creación del sello electrónico relacionados con los datos de validación del sello electrónico se encuentren en un dispositivo cualificado de creación de sellos electrónicos, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

7.1.1 Descripción del perfil

Los certificados seguirán el estándar X509, definido en la RFC 5280, y tendrán los siguientes campos descritos en esta sección:

Certificados emitidos por ACA – Trusted Certificates

CAMPOS	
Versión	V3
Nº Serie (Serial)	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)
Algoritmo de Firma	Sha1WithRSAEncryption
Emisor (issuer)	CN = ACA - Certificados Trusted OU = Autoridad de Certificación de la Abogacia O = Consejo General de la Abogacia NIF:Q-2863006I E = ac@acabogacia.org L = Madrid C = ES
Válido desde (notBefore)	(fecha de inicio de validez, tiempo UTC)
Válido hasta (notAfter)	(fecha de fin de validez, tiempo UTC)
Asunto (Subject)	(Según especificaciones de la sección 3.1.1)
Clave pública	RSA (1024 bits)

Certificados emitidos por ACA – Trusted Certificates 2014

CAMPOS	
Versión	V3
Nº Serie (Serial)	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)
Algoritmo de Firma	Sha1WithRSAEncryption
Emisor (issuer)	CN = ACA - Trusted Certificates - 2014 SERIALNUMBER = Q2863006I OU = Autoridad de Certificación de la Abogacia O = Consejo General de la Abogacia C = ES
Válido desde (notBefore)	(fecha de inicio de validez, tiempo UTC)
Válido hasta (notAfter)	(fecha de fin de validez, tiempo UTC)
Asunto (Subject)	(Según especificaciones de la sección 3.1.1)
Clave pública	RSA (2048 bits)

Certificados emitidos por ACA CA2

CAMPOS	
Versión	V3

Nº Serie (Serial)	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)
Algoritmo de Firma	Sha256WithRSAEncryption
Emisor (issuer)	CN = ACA CA2 OI = VATES-Q2863006I OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA O = CONSEJO GENERAL DE LA ABOGACIA C = ES
Valido desde (notBefore)	(fecha de inicio de validez, tiempo UTC)
Válido hasta (notAfter)	(fecha de fin de validez, tiempo UTC)
Asunto (Subject)	(Según especificaciones de la sección 3.1.1)
Clave pública	RSA (2048 bits)

7.1.2 Extensiones del certificado

Se incluirán las siguientes extensiones:

Certificados emitidos por ACA – Trusted Certificates

EXTENSIONES	
Nombre alternativo del emisor (IssuerAlternativeName)	Nombre RFC822=ac@acabogacia.org Dirección URL=http://www.acabogacia.org
Nombre alternativo del sujeto (SubjectAlternativeName)	Nombre RFC822=xxxx.xxxxx@cgae.es
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos
Uso mejorado de las claves (ExtendedKeyUsage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	5a f6 34 ce 96 76 56 b7 7c e9 dc dc 1d 13 6c 79 de 0f 30 76
Identificador de clave de asunto (SubjectKeyIdentifier)	
Bases de certificado (SubjectStatement)	Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.16533.20.3.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador:

	http://www.acabogacia.org/doc [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario
Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/acatrusted.crl http://crl.acabogacia.org/crl/acatrusted.crl
Restricciones básicas (BasicConstraints)	Tipo de asunto= Entidad final Restricción de longitud de ruta= Ninguno
Acceso a la Información de Autoridad (Authority Information Access)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL= http://www.acabogacia.org/certificados/ACAtrusted.crt
qcStatements x.509v3 certificate extension from RFC 3039	

Certificados emitidos por ACA – Trusted Certificates 2014

EXTENSIONES	
Nombre alternativo del sujeto (SubjectAlternativeName)	Opcional
Restricciones básicas (BasicConstraints)	Tipo de asunto= Entidad final Restricción de longitud de ruta= Ninguno
Identificador de clave del titular (SubjectKeyIdentifier)	
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	81 8F D1 63 00 4A CA 4D 20 97 A6 52 00 60 2E D2 CC 36 8B 6D
Uso mejorado de las claves (ExtendedKeyUsage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Acceso a la Información de Autoridad (Authority Information Access)	[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL= http://ocsp.redabogacia.org [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección

	URL= http://www.acabogacia.org/certificados/ACAtrustedV2.crt
Directivas de certificado (Certificate Policies)	Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.20.3.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc
Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/ACAtrustedV2.crl http://crl.acabogacia.org/crl/ACAtrustedV2.crl
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos, Contrato de claves

Certificados emitidos por ACA CA2

EXTENSIONES	VALOR
Nombre alternativo del sujeto (SubjectAlternativeName)	Opcional
Restricciones básicas (BasicConstraints)	Tipo de asunto= Entidad final Restricción de longitud de ruta= Ninguno
Identificador de clave del titular (SubjectKeyIdentifier)	
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	8A 15 1F AF 74 EF 1F 01 07 73 2A 90 2A 41 09 7E 1B 48 D0 C0
Uso mejorado de las claves (ExtendedKeyUsage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Acceso a la Información de Autoridad (Authority Information Access)	[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL= http://ocsp.redabogacia.org [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo:

	<p style="text-align: center;">Dirección</p> <p>URL=http://www.acabogacia.org/certificados/aca_ca2.crt</p>
Directivas de certificado (Certificate Policies)	<p>Directiva de certificados:</p> <p style="padding-left: 40px;">Identificador de directiva= 1.3.6.1.4.1.16533.20.3.1</p> <p>[1,1]Información de calificador de directiva:</p> <p style="padding-left: 40px;">Id. de calificador de directiva=CPS</p> <p>Certificador:</p> <p>http://www.acabogacia.org/doc</p>
Declaración de Certificados Calificados qcStatements x.509v3 certificate extension from RFC 3039	<p>1.- id-etsi-qcs-QcCompliance</p> <p>2.- id-etsi-qcs-QcPDS</p> <p style="padding-left: 40px;">URL=http://www.acabogacia.org/doc/EN</p>
Punto de distribución de la CRL (CRLDistributionPoint)	<p>http://www.acabogacia.org/crl/aca_ca2.crl</p> <p>http://crl.acabogacia.org/crl/aca_ca2.crl</p>
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Contrato de claves

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será

1. 2. 840. 113549. 1. 1. 11 SHA-256 with RSA Encryption

El identificador de objeto del algoritmo de la clave pública será

1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Restricciones de los nombres

No estipulado.

7.2. Perfil de CRL

7.2.1 Número de versión

Las CRL emitidas por la AC son de la versión 2.

7.2.2 Periodo de Emisión y validez

Se emiten de oficio diariamente y cuando sufra un cambio de estado. La validez es semanal.

7.2.3 Publicación.

La publicación es inmediata a su emisión.
Los puntos de distribución son:

Para Certificados emitidos por la CA ACA – Trusted Certificates

<http://www.acabogacia.org/crl/ACAtrusted.crl>
<http://crl.acabogacia.org/crl/ACAtrusted.crl>

Para Certificados emitidos por la CA ACA – Trusted Certificates 2014

<http://www.acabogacia.org/crl/ACAtrustedV2.crl>
<http://crl.acabogacia.org/crl/ACAtrustedV2.crl>

Para certificados emitidos con la ACA CA2

http://www.acabogacia.org/crl/aca_ca2.crl
http://crl.acabogacia.org/crl/aca_ca2.crl

7.2.4 CRL y extensiones

Se incluirán las siguientes extensiones

Extensiones
Versión
Fecha Inicio de Validez
Fecha Fin de Validez
Algoritmo de Firma
Número de Serie
Puntos de distribución

8. Especificación de la administración

8.1. *Autoridad de las políticas*

El CGAE es el responsable del mantenimiento de las políticas de certificación, y puede ser contactado en la dirección especificada en el apartado 1.

8.2. *Procedimientos de especificación de cambios*

Todos los cambios propuestos que puedan afectar sustancialmente a los usuarios de esta política serán notificados inmediatamente a los suscriptores mediante la publicación en la web de AC Abogacía, haciendo referencia expresa en la “página principal” de la misma a la existencia del cambio.

Los usuarios afectados podrán presentar sus comentarios a la organización de la administración de las políticas dentro de los 45 días siguientes a la recepción de la notificación.

8.3. *Publicación y copia de la política*

Una copia de esta Política estará disponible en formato electrónico en la dirección de Internet: <http://www.acabogacia.org/doc>. Las versiones anteriores serán retiradas de su consulta on-line, pero pueden ser solicitadas por los interesados en la AC Abogacía.

8.4. *Procedimientos de aprobación de la Política*

La publicación de las revisiones de esta política deberá ser aprobada por el CGAE.

ANEXO 1: Información técnica

En cumplimiento de lo establecido en la Ley de Firma Electrónica y eIDAS, se informa a los suscriptores y usuarios de determinados aspectos en relación con dispositivos de creación y de verificación de firma electrónica que son compatibles con los datos de firma y con el certificado expedido, así como de mecanismos considerados seguros para la creación y verificación de firmas.

1. Dispositivos del suscriptor

No estipulado.

2. Creación y verificación de firmas

2.1. Estándares y parámetros admitidos

No estipulado.

2.2. Métodos de verificación de firmas

La comprobación de la firma electrónica es imprescindible para determinar que fue generada por el poseedor de claves, utilizando la clave privada correspondiente a la clave pública contenida en el certificado del suscriptor, y para garantizar que el mensaje o el documento firmado no fue modificado desde la generación de la firma electrónica.

La comprobación se ejecutará normalmente de forma automática por el dispositivo del usuario verificador, y en todo caso, y de acuerdo con la Declaración de Prácticas de Certificación (CPS) y la legislación vigente, con los siguientes requerimientos:

- Es necesario utilizar un dispositivo apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizadas en el certificado y/o ejecutar cualquier otra operación criptográfica. Dichos dispositivos deberán cumplir lo dispuesto en el artículo 25 de la ley de Firma Electrónica
- Es necesario establecer la cadena de certificados en que se basa la firma electrónica que debe verificarse y asegurarse que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica. Es responsabilidad y decisión del usuario que verifica la elección de la cadena apropiada si hubiera más de una posible.
- Es necesario comprobar la integridad, la firma digital y el estado de validez (no caducado, no revocado o no suspendido) de todos los certificados de la cadena con la información suministrada por AC Abogacía en su servicio de publicación de certificados. Sólo se puede considerar correctamente verificada una firma electrónica si todos o cada uno de los certificados de la cadena son correctos y vigentes.

- Es necesario verificar que los certificados de la cadena se han usado dentro de las condiciones y límites de uso que impone el emisor de cada uno de ellos, y por firmantes autorizados. Cada certificado de la cadena de certificación dispone de información sobre sus condiciones de uso y enlaces a documentación sobre los mismos.
- Es necesario verificar la adecuación de los algoritmos y parámetros de firma de todos los certificados de la cadena y del propio documento firmado.
- Es necesario determinar la fecha y hora de generación de la firma electrónica, ya que la verificación correcta exige que todos los certificados de la cadena fueran vigentes en el momento de generación de la firma.
- Es necesario, finalmente, determinar los datos firmados y verificar técnicamente la propia firma electrónica respecto del certificado utilizado para firmar, asociado a una cadena de certificación válida.

El usuario que verifica una firma debe actuar con la máxima diligencia antes de confiar en los certificados y las firmas digitales, y utilizar un dispositivo de verificación de firma electrónica con la capacidad técnica, operativa y de seguridad suficiente para ejecutar el proceso de verificación de firma correctamente.

Por último, los requisitos para la validación de firmas electrónicas cualificadas vienen determinados en el artículo 32 del Reglamento 910/2014 (eIDAS).

El usuario que verifica será el responsable exclusivo del daño que pueda sufrir por la incorrecta elección del dispositivo de verificación, salvo que éste hubiere sido proporcionado por AC Abogacía.

El usuario que verifica tiene que tener en cuenta las limitaciones de uso del certificado indicadas de cualquier manera en el certificado, incluyendo aquellas no procesadas automáticamente por el dispositivo de verificación e incorporadas por referencia. Si las circunstancias requieren garantías adicionales, el verificador deberá obtener estas garantías para que la confianza sea razonable.

En cualquier caso, la decisión final respecto a confiar o no en una firma electrónica verificada es exclusivamente del usuario.

2.3. Verificación de la Firma Electrónica a lo largo del tiempo

Si el usuario desea disponer de garantías a lo largo del tiempo que le permitan comprobar la validez de una firma electrónica, debe utilizar mecanismos adicionales, entre otros:

- Si el Firmante ha generado la firma en un formato capaz de verificarse a lo largo del tiempo, como los definidos en la norma EN 319 122-2 “Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures” del European Telecommunications Standards Institute (www.etsi.org), que AC Abogacía recomienda.

- Utilización por el firmante y el verificador de servicios de mediación de terceras partes, en los que ambos depositen su confianza, como:
 - Servicios de validación de certificados
 - Servicios de sellado de tiempo
 - Servicios de notarización de transacciones
 - Etc
- Conservación, de manera segura e íntegra, junto con la firma de todos los datos necesarios para su verificación:
 - Todos los certificados de la cadena de certificación.
 - Todas las CRL vigentes inmediatamente antes y después del momento de la firma.
 - Las políticas y prácticas en vigor en el momento de la firma.

ANEXO 2: ACRONIMOS

AC	Autoridad de Certificación, también puede encontrarse identificada por el acrónimo CA (<i>Certification Authority</i>)
ACA	Autoridad de Certificación de la Abogacía
AR	Autoridad de Registro también puede encontrarse identificada por el acrónimo RA (<i>Registration Authority</i>)
ARL	<i>Authority Revocation List</i> , lista de certificados revocados de la Autoridad de Certificación Raíz
CGAE	Consejo General de la Abogacía Española
CPS	<i>Certification Practice Statement</i> , Declaración de Prácticas de Certificación. también puede encontrarse identificada por el acrónimo DPC
CRL	<i>Certificate revocation list</i> , Lista de certificados revocados
CSR	<i>Certificate Signing request</i> , petición de firma de certificado
DES	<i>Data Encryption Estándar</i> . Estándar de cifrado de datos
DN	<i>Distinguished Name</i> , nombre distintivo dentro del certificado digital
DSA	<i>Digital Signature Algorithm</i> . Estándar de algoritmo de firma
DSCF/	Dispositivo Seguro de Creación de Firma
DCCFE	Dispositivo Cualificado de Creación de Firmas Electrónicas
eIDAS	Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
FIPS	<i>Federal information Processing Estándar publication</i>
IETF	<i>Internet Engineering task force</i>
ICA	Ilustre Colegio de Abogados
ISO	<i>International Organisation for Standardization</i> . Organismo internacional de estandarización
ITU	<i>International Telecommunications Union</i> . Unión Internacional de Telecomunicaciones.
LDAP	<i>Lightweight Directory Access Protocol</i> . Protocolo de acceso directorio
OCSP	<i>On-line Certificate Status Protocol</i> . Protocolo de acceso al estado del Certificado
OID	<i>Object identifier</i> . Identificador de Objeto
PA	<i>Policy Authority</i> . Autoridad de la Política
PC	Política de Certificación puede encontrarse identificada por el acrónimo CP (<i>Certification Policy</i>)
PIN	<i>Personal Identification Number</i> , Número de identificación personal
PKI	<i>Public Key Infrastructure</i> , Infraestructura de clave pública
PUK	<i>Personal Unblocking Key</i> , Código de desbloqueo
RSA	<i>Rivest-Shimmar-Adleman</i> . Tipo de algoritmo de cifrado
SHA-256	<i>Secure Hash Algorithm</i> . Algoritmo seguro de Hash
TSL	<i>Transport Layer Security Su antecesor es SSL (Secure Socket Layer</i> . Protocolo diseñado por Netscape y convertido en estándar en la Red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor)
TCP/IP	<i>Transmission Control Protocol/Internet Protocol</i> Sistema de Protocolos, definidos en el marco de la IETFT. El Protocolo TCP se usa para dividir en

origen la información en paquetes, para luego recomponerla en destino, el Protocolo IP se encargará de direccionar adecuadamente la información hacia su destinatario.