

Autoridad de Certificación de la Abogacía



Referencia: **CP1_ACA_005.0**

Fecha: **30/10/2006**

Estado del documento: **Publicado**



**Consejo General de la
Abogacía Española**

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

CP1_ACA_005.0

CERTIFICADOS CORPORATIVOS RECONOCIDOS DE COLEGIADO

(VERSIÓN 005.0)

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 |
|--------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 27/03/2003 | CP001_ACA_001.0 | Versión inicial |
| 02/03/2004 | CP001_ACA_001.1 | Corrección erratas. |
| 26/10/2004 | CP1_ACA_002.0 | Revisión general. Modificaciones para mejor adecuación a lo dispuesto en la Ley 59/2003 de Firma Electrónica y mayor claridad para suscriptores y usuarios. |
| 01/09/2005 | CP1_ACA_003.0 | Actualización nuevo certificado raíz. |
| 13/03/2006 | CP1_ACA_003.0 | Revisión general |
| 13/07/2006 | CP1_ACA_004.0 | Inclusión de OID para referenciar a la CPS de aplicación |
| 30/10/2006 | CP1_ACA_005.0 | Modificación perfil del certificado |
| | | |

Índice de Contenido

| | | |
|-----------|--------------------------------------------------------------------------|-----------|
| 1. | <i>Introducción</i> | 5 |
| 1.1. | Vista General | 5 |
| 1.2. | Identificación | 6 |
| 1.3. | Comunidad y Ámbito de Aplicación. | 6 |
| 1.4. | Datos de contacto | 9 |
| 2. | <i>Cláusulas Generales</i> | 10 |
| 2.1. | Obligaciones | 10 |
| 2.2. | Responsabilidad | 10 |
| 2.3. | Responsabilidad financiera | 11 |
| 2.4. | Interpretación y ejecución | 12 |
| 2.5. | Tarifas | 12 |
| 2.6. | Publicación y Registro de Certificados | 13 |
| 2.7. | Auditorias | 14 |
| 2.8. | Confidencialidad y Protección de Datos Personales | 14 |
| 2.9. | Derechos de propiedad intelectual | 15 |
| 3. | <i>Identificación y Autenticación</i> | 16 |
| 3.1. | Registro inicial | 16 |
| 3.2. | Renovación de certificados | 19 |
| 3.3. | Reemisión después de una revocación | 20 |
| 3.4. | Solicitud de revocación | 20 |
| 4. | <i>Requerimientos Operacionales</i> | 21 |
| 4.1. | Solicitud de certificados | 21 |
| 4.2. | Emisión de certificados | 22 |
| 4.3. | Aceptación de certificados | 22 |
| 4.4. | Suspensión y Revocación de certificados | 22 |
| 4.5. | Procedimientos de Control de Seguridad | 22 |
| 5. | <i>Controles de Seguridad Física, Procedimental y de Personal</i> | 23 |
| 6. | <i>Controles de Seguridad Técnica</i> | 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 | 26 |
| 6.4. | Ciclo de vida de los dispositivos criptográficos | 26 |
| 6.5. | Controles de seguridad | 26 |
| 6.6. | Controles de ingeniería de los módulos criptográficos | 26 |
| 7. | <i>Perfiles de Certificado</i> | 27 |
| 7.1. | Perfil de Certificado | 27 |
| 7.2. | Perfil de CRL | 30 |

| | |
|--------------------------------------------------|-----------|
| 8. Especificación de la administración | 31 |
| 8.1. Autoridad de las políticas | 31 |
| 8.2. Procedimientos de especificación de cambios | 31 |
| 8.3. Publicación y copia de la política | 31 |
| 8.4. Procedimientos de aprobación de la Política | 31 |
| ANEXO 1: Información técnica | 32 |
| Dispositivos del suscriptor | 32 |
| Creación y verificación de firmas | 33 |
| Anexo 2: ACRONIMOS | 36 |

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 presente documento especifica la Política de Certificación del Certificado digital denominado “Certificado Corporativo Reconocido de Colegiado” o simplemente “Certificado de Colegiado” 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 (Directiva 1999/93/CE) y en España (Ley 59/2003 de 19 de Diciembre, de Firma Electrónica), cumpliendo todos los requisitos técnicos y de seguridad exigidos para emisión de Certificados Reconocidos y está basada en la especificación del estándar RCF 2527 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*.

La 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

| | |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Nombre: | CP1_ACA_005.0 |
| O.I.D. | 1.3.6.1.4.1.16533.10.2.1 |
| Descripción: | Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: certificados corporativos reconocidos de Colegiado |
| Versión: | 005.0 |
| Fecha de Emisión: | 26/10/2006 |
| 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, vinculando una determinada clave pública con una persona (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, las AR's son las siguientes entidades:

- a) El Consejo General de la Abogacía Española (CGAE)
- b) Los Consejos Autonómicos de la Abogacía
- c) Los Colegios de Abogados

Registrador exclusivo para certificados corporativos de colegiado. Sólo los Colegios de Abogados pueden ser Registradores para sus colegiados, debido a que los Colegios de

Abogados poseen la capacidad certificadora en exclusiva, acerca de la condición de abogado.

1.3.3 Prestador de servicios de certificación (PSC).

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.

1.3.4 Suscriptor

Bajo esta Política el Suscriptor es una persona física, perteneciente a un Colegio de Abogados de España en calidad de colegiado del mismo, poseedor de un “Certificado Reconocido de Colegiado” alojado en un dispositivo seguro de creación de firma. El suscriptor recibe también el nombre de “Firmante”, según se define el art. 6 de la Ley 59/2003

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 acreditación de la autenticidad e integridad del documento firmado y en consecuencia se sujeta a lo dispuesto en esta Política, en las CPS aplicables 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 reconocido de Colegiado.

1.3.7 Ámbito de Aplicación y Usos

El Certificado emitido bajo la presente Política, permite identificar a una persona física en el ámbito de su actividad profesional. Los certificados de colegiado podrán usarse en los términos establecidos por las prácticas de certificación correspondientes.

Además de las simples comunicaciones electrónicas, se autoriza su utilización para transacciones comerciales, económicas y financieras, en medio digital, siempre que basados en el estándar RCF 3647 (X. 509), y que no excedan el valor máximo definido en la CPS, que nunca podrá ser inferior a lo dispuesto en esta política.

El Certificado emitido bajo esta Política puede ser utilizado con los siguientes propósitos:

- Identificación del firmante y su vinculación con el Colegio Profesional: El Suscriptor del Certificado puede autenticar, frente a otra parte, su identidad y su vinculación al Colegio Profesional, demostrando la asociación de su clave privada

con la respectiva clave pública, contenida en el Certificado. El suscriptor podrá identificarse válidamente ante cualquier persona mediante la firma de un e-mail o cualquier otro fichero.

- Integridad del documento firmado: La utilización de este Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Suscriptor. Se certifica que el mensaje recibido por el Usuario es el mismo que fue emitido por el Suscriptor
- No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Suscriptor que ha firmado no puede negar la autoría o la integridad del mismo.
- A pesar de ser posible su utilización para la encriptación de datos, no se recomienda la misma debido a que, no es posible la recuperación de los datos encriptados en caso de pérdida de la clave privada por parte del Suscriptor. El Suscriptor o el Usuario lo harán, en todo caso, bajo su propia responsabilidad.

Los certificados descritos en esta política son certificados reconocidos de acuerdo con lo establecido en el art. 11 de la Ley 59/2003. Corresponden a certificados reconocidos (en su caso con dispositivo seguro de creación de firma electrónica), expedidos al público, de acuerdo con la norma técnica TS 101 456 v1.2.1, del Instituto Europeo de Normas de Telecomunicaciones.

Los certificados de colegiado deben emplearse necesariamente con un dispositivo seguro de creación de firma electrónica, que cumpla los requisitos establecidos por el art. 24 de la Ley 59/2003 y esta política. Garantizan la identidad del suscriptor y del poseedor de la clave privada de firma, resultando idóneos para ofrecer soporte a la firma electrónica reconocida; esto es, la firma electrónica avanzada que se basa en certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo que, de acuerdo con el art. 3 de la Ley 59/2003, se equipara a la firma manuscrita por efecto legal, sin necesidad de cumplir requisito adicional alguno.

1.3.7.1 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 Prácticas 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.

La AC no crea, almacena ni posee en ningún momento la clave privada del suscriptor, no siendo posible recuperar los datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor.

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 encriptación 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

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 y la Ley 59/2003, donde sean aplicables

2.1.2 AR

Las Autoridades de Registro son delegadas por la CA 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 como AC responderá de acuerdo con el régimen de responsabilidad que establece la Ley 59/2003, de Firma Electrónica 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 las AR's se exonerarán de su responsabilidad en los términos establecidos en la CPS y las políticas de certificación. En particular, la AC y las AR's no serán responsables en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de fuerza mayor.
2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente 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.
3. Por el uso indebido o fraudulento de los certificados o CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.
4. Por el uso indebido de la información contenida en el Certificado o en la CRL.
5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Usuarios en la normativa vigente, la presente CPS o en la Política de Certificación correspondiente.
6. Por el contenido de los mensajes o documentos firmados.
7. Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.
8. 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 de servicios de Certificación dispone de 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 PSC tal como se define en la legislación española vigente.

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 practicas 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:
 - o Los certificados emitidos o en trámite de emisión.
 - o La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación.
 - o 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 regirán 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.501.

El DN de los certificados Corporativos 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 Unidad en la Organización –OU
- Un componente Título-T
- Un componente de ubicación geográfica -ST
- Un componente Estado (Country)-C
- Un componente Número de Serie –serialNumber
- Un componente Nombre de Pila (Given name)- G
- Un componente Apellido 1 “Surname” – SN
- Un componente Apellido 2 con OID 1.3.6.1.4.1.16533.30.1

Certificados de Colegiado

- El valor autenticado del componente Nombre (Common Name) –CN contendrá el nombre (Nombre y Apellidos) y número de NIF o NIE del suscriptor
- El valor autenticado del componente E-mail –E contendrá la dirección de correo electrónico del suscriptor

- El valor autenticado del componente Organización –O contendrá el nombre del Registrador, es decir el Colegio de Abogados al que pertenezca el suscriptor, y una referencia al código identificativo de la AR
- El valor autenticado del componente Unidad en la Organización –OU contendrá el Código postal de la sede principal del registrador y el numero de colegiado del suscriptor
- El valor autenticado del componente Título-T contendrá el titulo o especialidad que estará condicionado a tres estados del Colegiado:
 - **Abogado:** que identifica al Colegiado que, al amparo del Art. 6 y siguientes del Estatuto General de la Abogacía Española, aprobado por Real Decreto 658/2001, de 22 de junio, ejerce profesionalmente la dirección y defensa de las partes en toda clase de procesos, o el asesoramiento y consejo jurídico.
 - **Colegiado no ejerciente:** que identifica al Colegiado que no actúa como abogado.
 - **Abogado inscrito:** identifica a aquellos abogados de otros Estados miembros que ejerzan en España al amparo de lo dispuesto en el Real Decreto 936/2001, de 3 de agosto, por el que se regula el ejercicio permanente en España de la profesión de abogado con título profesional obtenido en otro Estado miembro de la Unión Europea.
- El valor autenticado del componente de ubicación geográfica -ST contendrá la población donde se encuentre la sede principal de la RA.
- El valor autenticado del componente Estado (Country)-C contendrá “ES”
- El valor autenticado del componente Número de Serie –serialNumber contendrá el NIF o NIE del suscriptor.
- El valor autenticado del componente Nombre de Pila (Given name)- G contendrá el nombre de pila del Suscriptor
- El valor autenticado del componente Apellido 1 “Surname” –SN contendrá el primer apellido del Suscriptor
- El valor autenticado del componente con OID 1.3.6.1.4.1.16533.30.1 contendrá el segundo apellido del Suscriptor

3.1.2 Pseudónimos

Los certificados corporativos de colegiado no admiten seudónimos. Tampoco se pueden emplear seudónimos para identificar a una organización.

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 del e-mail, el número de colegiado y/o el NIF se usarán 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 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 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 estipulado

3.1.7 Métodos de prueba de la posesión de la clave privada

La clave privada será generada por el suscriptor y permanecerá en todo momento en posesión exclusiva del mismo.

El método de prueba de la posesión de la clave privada por el suscriptor será PKCS#10.

3.1.8 Autenticación de la identidad de un individuo

Para realizar una correcta verificación de la identidad del suscriptor de certificados personales, se exigirá la personación física del suscriptor 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.

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.

Lo dispuesto en los párrafos anteriores podrá no ser exigible en certificados emitidos con posterioridad a la entrada en vigor de la Ley 59/2003 de Firma Electrónica, en los siguientes casos:

- a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la AR en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en el párrafo primero y el período de tiempo transcurrido desde la identificación es menor de cinco años.
- b) Cuando para solicitar un certificado se utilice otro para cuya expedición se hubiera identificado al firmante en la forma prescrita en el párrafo primero y le conste a la AR que el período de tiempo transcurrido desde la identificación es menor de cinco años.

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.

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, en cuyo caso deberá facilitar la clave de revocación que se le entregó junto con el certificado, o deberá identificarse ante la AR según lo establecido en el apartado correspondiente.
- Los operadores autorizados de la AR del suscriptor.
- 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 establecido por la CPS , y se procederá en la forma allí descrita a realizar y tramitar las solicitudes de revocación.

4. Requerimientos Operacionales

4.1. Solicitud de certificados

Las AR's gestionan las solicitudes de Certificados de Colegiado y Certificados de Personal Administrativo.

La solicitud de un certificado digital podrá realizarse de las siguientes formas:

- On Line: El solicitante accediendo a la página web <http://www.acabogacia.org> en el apartado de Solicitud On-line, podrá solicitar a su Autoridad de Registro la realización de un certificado digital, el sistema enviara un correo electrónico a los Operadores autorizados de la AR, comunicando esta solicitud. La AR comunica al solicitante la disponibilidad para realizar el proceso de registro
- Personándose en su Colegio de Abogados 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, convirtiéndose el solicitante en suscriptor.

La AR le hace entrega (si no dispone de él) de un kit conteniendo el dispositivo criptográfico de soporte de la clave privada y los dispositivos de acceso a el, si los hubiera

Si el dispositivo no hubiere sido previamente inicializado, el suscriptor inicializa en la propia AR y ante el operador el dispositivo criptográfico. Durante el proceso de inicialización se generan los datos de activación del dispositivo y de acceso a la clave privada que contendrá. El suscriptor generará los datos de activación, o si la inicialización se produce en una entidad externa, le serán entregados mediante un proceso que asegure la confidencialidad de los mismos ante terceros. La inicialización del dispositivo elimina totalmente cualquier información previa contenida en el mismo.

A continuación, el suscriptor genera el par de claves y un CSR en su dispositivo criptográfico, enviando por un canal seguro la clave publica junto con los datos verificados a la AC en formato PKCS10 u otro equivalente. La generación del par de claves exigirá la introducción correcta de los datos de activación del dispositivo, y la introducción de un código de identificación del dispositivo que lo relaciona con el suscriptor autorizado a utilizarlo.

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, mediante la firma digital de la petición con su certificado de operador. 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, si la petición recibida no contiene errores técnicos, en el formato o contenido de la misma, vinculando de forma segura el certificado con la información de registro, incluyendo la clave pública certificada, en un sistema que utiliza protección contra falsificación y mantiene la confidencialidad de los datos intercambiados.
- El certificado generado es enviado de forma segura a la AR. Para proceder a su descarga en el Dispositivo Criptográfico en presencia del Suscriptor.
- La AC notifica al suscriptor la emisión del mismo.
- El certificado generado es enviado de forma segura al Registro de Certificados, que lo pone a disposición de los usuarios. Aceptación de certificados

Con la entrega de la tarjeta Colegial el suscriptor acepta su certificado en el dispositivo criptográfico que custodia la clave privada.

4.3. Aceptación de certificados

Se considerará que un suscriptor acepta su certificado cuando descarga el certificado en su dispositivo criptográfico que custodia la clave privada, mediante el acceso al sistema de descarga de certificados de la AC-AR y efectúa los pasos técnicos que el sistema provee para la descarga.

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

Las claves de los suscriptores y operadores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 2, ITSEC High4 u otro de nivel equivalente.

Los dispositivos criptográficos de custodia de la clave privada del suscriptor u operador aportan un nivel de seguridad igual o superior al establecido por la legislación vigente para dispositivos de creación de los datos de firma. La norma europea de referencia para los dispositivos de suscriptor utilizados es CEN CWA 14169.

El dispositivo criptográfico utiliza una clave de activación para el acceso a las claves privadas. En caso de que la entrega del dispositivo no se realice de manera presencial en la AR, los datos de activación se enviarán al lugar de entrega por separado de los dispositivos.

Las claves son generadas usando el algoritmo de clave pública RSA, con los adecuados parámetros. Las claves tienen una longitud mínima de 1024 bits.

6.1.2 Entrega de la clave pública al emisor del certificado

El envío de la clave pública a la AC para la generación del certificado se realiza mediante formato estándar PKCS#10

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 de 1024 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 3 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 los suscriptores y operadores son generadas por el propio suscriptor de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 2, ITSEC High4 u otro de nivel equivalente.

Los dispositivos criptográficos de custodia de la clave privada del suscriptor u operador aportan un nivel de seguridad igual o superior al establecido por la legislación vigente para dispositivos de creación de los datos de firma. La norma europea de referencia para los dispositivos de suscriptor es CEN CWA 14169.

Las claves de las CA vinculadas son generadas en un módulo criptográfico nCipher modelo nShield validado FIPS 140-1 nivel 3.

6.1.8 Fines del uso de la clave

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

6.2. Protección de la clave privada

Clave privada de la AC

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

Clave privada del suscriptor

La clave privada del suscriptor se mantendrá en un dispositivo criptográfico y será controlada y gestionada por el suscriptor. Tendrá un sistema de protección contra intentos de acceso que bloqueen el dispositivo cuando se introduzca sucesivas veces un código de acceso erróneo.

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 criptográficos seguro de creación de firma (DSCF)

Se empleará como DSCF tarjetas con criptoprocador para que el suscriptor genere y almacene los datos de creación de firma, es decir la clave privada:

- a) Las tarjetas son preparadas y estampadas por un proveedor externo de la tarjeta.
- b) La gestión de distribución del soporte la realiza el proveedor externo de tarjetas que lo distribuye a las autoridades de registro para su entrega personal al suscriptor. La AR puede realizar una personalización gráfica de la tarjeta.
- c) El suscriptor inicializa la tarjeta y la utiliza para generar el par de claves y enviar la clave pública a la CA.
- d) La CA envía un certificado de clave pública al suscriptor que es introducido en la tarjeta.
- e) La tarjeta es reutilizable y puede mantener de forma segura varios pares de claves.

El periodo de vida útil de las tarjetas de usuario tendrá una vida media de 6 años

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 3280 "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*", ETSI TS 101 862 conocida como "*European profile for Qualified Certificates*" y la RFC 3739 (que sustituye a RFC 3039) "*Qualified Certificates Profile*". En caso de contradicción prevalecerá lo dispuesto en la norma TS 101 862.

Los certificados corporativos definidos en esta Política son **certificados reconocidos**, de acuerdo con lo establecido en art. 11 de la Ley 59/2003, con el contenido prescrito por el art. 11 de la Ley 59/2003, y expedidos en un dispositivo que sigue las definiciones del art. 24 de la Ley 59/2003. Los certificados que corresponden a certificados reconocidos lo son de acuerdo con lo definido en los apartados 5.2 y 5.3 de la especificación técnica TS 101 456 del Instituto Europeo de Normas de Telecomunicaciones (ETSI).

Los certificados reconocidos incluirán, al menos, los siguientes datos:

- a) La indicación de que se expiden como tales.
- b) El código identificativo único del certificado.
- c) La identificación de la AC que expide el certificado y su domicilio.
- e) La identificación del suscriptor según lo estipulado en el apartado 3.1.1. en el campo DN del certificado.
- g) El comienzo y el fin del período de validez del certificado.
- h) Los límites de uso del certificado, si se establecen.
- i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

7.1.1 Descripción del perfil

Los certificados seguirán el estándar X509, definido en la RFC 3280, y tendrán los siguientes campos descritos en esta sección:

| 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 Corporativos OU = Autoridad de Certificación de la Abogacía O = Consejo General de la Abogacía NIF:Q-2863006I E = ac@acabogacia.org L = Madrid C = ES |
| Valido desde (notBefore) | (fecha de inicio de validez, tiempo UTC) |
| Valido hasta (notAfter) | (fecha de fin de validez, tiempo UTC) |
| Asunto (Subject) | (Según especificaciones de la sección 3.1.1) |
| Clave pública | RSA (1024 bits) |

7.1.2 Extensiones del certificado

Se incluirán las siguientes extensiones:

| 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, Contrato de claves |
| 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) |
| Tipo de certificado Netscape (NetscapeCertType) | Autenticación del cliente SSL, SMIME (a0) |
| URL de directiva de entidad emisora de certificados de Netscape | http://www.acabogacia.org/doc |

| | |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (netscape-ca-policy-url) | |
| Comentario de Netscape (NetscapeComment) | Este es un certificado personal reconocido. Consulte http://www.acabogacia.org/doc |
| Identificador de clave de entidad emisora (AuthorityKeyIdentifier) | 5a794ca10cfc08162cc285454f 32abe72b45c011 |
| Identificador de clave de asunto (SubjectKeyIdentifier) | |
| Bases de certificado (SubjectStatement) | <p>Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.16533.10.2.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://www.acabogacia.org/doc</p> <p>[1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Texto de aviso=Este es un certificado personal reconocido. Consulte http://www.acabogacia.org/doc</p> |
| Punto de distribución de la CRL (CRLDistributionPoint) | http://www.acabogacia.org/crl/acacorporativos.crl http://crl.acabogacia.org/crl/acacorporativos.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/ACAcorporativos.crt |
| 1.3.6.1.5.5.7.1.3 qcStatements x.509v3 certificate extension from RFC 3039 | 0 Euros |

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. 5 SHA-1 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:

<http://www.acabogacia.org/crl/ACAcorporativos.crl>
<http://crl.acabogacia.org/crl/ACAcorporativos.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 |
| Numero de Serie |
| Puntos de distribucion |

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 59/2003 de Firma Electrónica, 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.

Dispositivos del suscriptor

Previo a la solicitud y emisión del certificado reconocido, el suscriptor deberá disponer del correspondiente dispositivo de generación de datos de creación de firmas y de creación de firmas.

A. Dispositivos Seguros de Creación de Firma:

Los Certificados Reconocidos identificados por el OID de Política 1.3.6.1.4.1.16533.10.2.1 requieren, para su emisión que los datos de creación de firma hayan sido generados por el suscriptor y se custodien en un dispositivo que cumple lo establecido en el artículo 24.3 de la Ley 59/2003, y que se denominan “Dispositivos seguros de Creación de Firma (DSCF)”.

La firma electrónica avanzada generada con tales dispositivos, y basada en un certificado reconocido, se denomina “Firma Electrónica Reconocida”, y tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

La AC considera adecuados los dispositivos que cumplan lo siguiente:

- Que hayan sido homologados como tales por la AC, para lo cual se requerirá una declaración del Fabricante o Importador en tal sentido, junto con la aportación de la documentación técnica pertinente, y la realización de las pruebas que se estimen convenientes durante el proceso de homologación..
- Que dispongan de la correspondiente certificación de dispositivo según lo establecido en el artículo 27 de la Ley 59/2003, en cuyo caso se admitirá sin más.

B. Otros Dispositivos de Creación de Firma:

No estipulado

En ambos casos (A) y (B), la AC sólo emitirán certificados respondiendo a las solicitudes que cumplan con lo establecido en el apartado siguiente para los algoritmos de generación de clave y parámetros del algoritmo de firma considerados adecuados (Claves RSA de 1024 bits) aunque el dispositivo disponga de la capacidad técnica para generar otro tipo de conjunto de parámetros de firma.

Creación y verificación de firmas

Estándares y parámetros admitidos

El uso correcto de los dispositivos para la creación de Firmas Electrónicas consideradas seguras, queda asociado a la utilización de un subconjunto de estándares y parámetros de entre los aprobados por la ETSI en el documento “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures” ETSI SR 002 176 (www.etsi.org)

| Identificación del conjunto | Algoritmo de firma | Parámetros del Algoritmo de Firma (long. Clave) | Algoritmo de Generación de clave | Método de relleno | Función de hash |
|-----------------------------|--------------------|-------------------------------------------------|----------------------------------|-------------------|-----------------|
| 001 | rsa | MinModLen=1020 | rsagen1 | emsa-pkcs1-v1_5 | sha1 |
| 002 | rsa | MinModlen=1020 | rsagen1 | emsa-pss | sha1 |
| 003 | rsa | MinModLen=1020 | rsagen1 | emsa-pkcs-v1_5 | ripemd160 |
| 004 | rsa | MinModLen=1020 | rsagen1 | emsa-pss | ripemd160 |

El método adecuado para la generación de números aleatorios para el algoritmo de generación de clave del cuadro anterior es:

| Algoritmo de Generación de clave | Algoritmo de firma | Método de generación de números aleatorios (RNG) | Parámetros del RNG |
|----------------------------------|--------------------|--------------------------------------------------|--------------------------------|
| rsagen1 | rsa | trueran or pseuran | EntropyBits≥128 or SeedLen≥128 |

Los terceros que confían en las firmas generadas deben asegurarse de que la firma recibida cumple con lo dispuesto en los párrafos anteriores.

En caso de que el dispositivo de creación de firmas permita efectuar diferentes tipos de firmas o la exportación de los datos de creación de firma a otro dispositivo que pudiese generar firmas electrónicas con parámetros distintos de los especificados (como podría ser una firma con de tipo “rsa” con función de hash “md5”), se informa a suscriptores y usuarios que dichas firmas no pueden ser consideradas seguras, quedando bajo la responsabilidad de los primeros el asegurarse de que se cumplen las prescripciones anteriores, y de los segundos de que las firmas recibidas son adecuadas técnicamente.

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 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.

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.

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 ETSI TS 101 733 “Electronic signature formats” 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:
 - o Servicios de validación de certificados
 - o Servicios de sellado de tiempo
 - o Servicios de notaría de transacciones
 - o Etc
- Conservación, de manera segura e íntegra, junto con la firma de todos los datos necesarios para su verificación:
 - o Todos los certificados de la cadena de certificación.
 - o Todas las CRL vigentes inmediatamente antes y después del momento de la firma.
 - o 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 |
| 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-1 | <i>Secure Hash Algorithm</i> . Algoritmo seguro de Hash |
| SSL | <i>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 |