Abogacía Española
CONSEJO GENERAL

AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

Certificados cualificados de autorizado

Política de Certificación (CP7_ACA_CA2_005.0)

Documento Público

CONTROL DE VERSIONES

Versión	Fecha	Descripción / Cambios Relevantes
27/06/2016	CP7_ACA_CA2_001	Versión inicial
03/05/2017	CP7_ACA_CA2_002	Se realizan las siguientes modificaciones del perfil del certificado: Se incluye el qctype Se modifica el KeyUsage para alinearlo con el ETSI EN 319 412 incluyendo no repudio, firma digital y cifrado de clave
02/06/2020	CP7_ACA_CA2_003	Adecuación RFC 3647 Se referencia todo lo relativo a Otros temas Operativos y Legales (punto 9) a la CPS
02/07/2020	CP7_ACA_CA2_004	Se separa en un campo independiente con OID 1.3.6.1.4.1.16533.30.3 el código identificativo de la RA
31/05/2022	CP7_ACA_CA2_005	Cambio de plantilla del documento Eliminación apartados duplicados con la CPS Adecuación legislativa Ley 6/2020, de 11 de noviembre Actualización acrónimos Actualización OID 1.3.6.1.4.1.16533.30.2

ÍNDICE

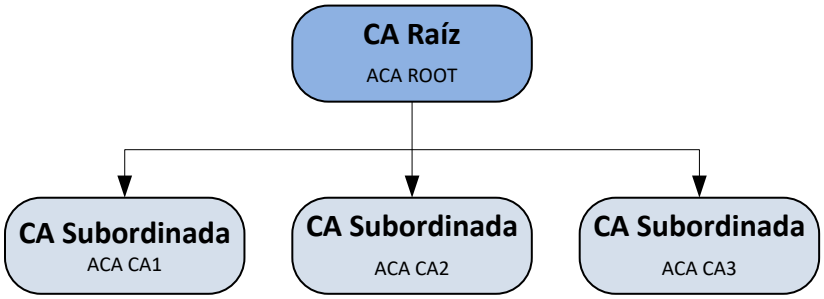
1. Introducción

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 Confianza mediante la creación de una jerarquía PKI propia. En cumplimiento 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.

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



El presente documento especifica la Política de Certificación del Certificado digital denominado "Certificado Cualificado de Autorizado" emitido por la autoridad de certificación del Consejo General de la Abogacía Española, o AC Abogacía. Durante la transición a la nueva jerarquía 2016, la jerarquía de 2014 indicada en la Declaración de Prácticas de Certificación (CPS) podrá emitir este tipo de certificados.

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 autorizadas o que representan a dichas organizaciones, por Prestadores de Certificación Acreditados.

Esta Política de Certificación está en conformidad con el REGLAMENTO (UE) No 910/2014, 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 (de aquí en adelante Reglamento 910/2014), la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante la Ley 6/2020) y las demás normas técnicas que regulan la identidad digital y los servicios de firma cualificada, 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.

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 del documento

Nombre:	CP7_ACA_CA2_005
O.I.D.	1.3.6.1.4.1.16533.20.6.1
Descripción:	Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: Certificado Cualificado de Autorizado
Versión:	005.0
Fecha de Emisión:	31/05/2022
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) 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

1.3.3. Suscriptor

Bajo esta Política el Suscriptor es una persona física, autorizada a solicitar un certificado digital ACA por un Despacho de Abogados, un Abogado, un Colegio de Abogados de España, Consejo de Colegios o el Consejo General de la Abogacía o instituciones vinculadas, que es poseedor de un dispositivo seguro de creación de firma asociada a un "Certificado Cualificado de Autorizado" alojado en un dispositivo cualificado de creación de firma electrónica. El suscriptor recibe también el nombre de "Firmante", según se define el art. 3.9 del Reglamento 910/2014..

1.3.4. 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 la Declaración de Prácticas de Certificación (CPS) aplicable y la legislación vigente, por lo que no se requerirá acuerdo posterior alguno.

1.3.5. Otros participantes

No estipulado.

1.4. Ámbito de Aplicación y Usos

1.4.1. Usos permitidos de los certificado

El Certificado emitido bajo la presente Política, permite identificar a una persona física a título personal y en el ámbito de su actividad relacionada con el "Autorizante" pudiendo ser éste a efectos de la presente política, un Despacho de Abogados, un Abogado, un Colegio de Abogados de España, Consejo de Colegios o el Consejo General de la Abogacía o instituciones vinculadas a la Abogacía. Los certificados Cualificados de Autorizado podrán usarse en los términos establecidos por las prácticas de certificación correspondientes.

Este Certificado digital se podrá utilizar de forma no exclusiva para identificar a las personas que acceden a la plataforma Lexnet Abogacía de forma que puedan acceder al buzón virtual de los abogados que los autoricen de forma expresa para ello y poder descargarse notificaciones y enviar escritos en su nombre.

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 Declaración de Prácticas de Certificación (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: El Suscriptor del Certificado puede autenticar, frente a otra parte, su identidad, 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 integro, 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 el cifrado de datos, no se recomienda la misma debido a que, no es posible la recuperación de los datos cifrados 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 Cualificados de Autorizado no identifican ni vinculan frente a terceros al Autorizante si no al suscriptor que conste en los mismos. No presuponen ningún tipo de apoderamiento de la persona física (Suscriptor) respecto de la persona física o jurídica Autorizante.

Los certificados descritos en esta política son certificados cualificados, que además son conformes con lo establecido en el artículo 51 deReglamento 910/2014, que establece en el apartado segundo que, los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/CE se considerarán Certificados Cualificados de firma electrónica con arreglo al presente Reglamento hasta que caduquen. Estos certificados sirven de base para la generación de firmas electrónicas cualificadas creadas mediante un dispositivo cualificado de creación de firmas electrónicas.

.

Los certificados Cualificados de Autorizado deben emplearse necesariamente con un dispositivo cualificado de creación de firma electrónica de acuerdo con la legislación de aplicación y esta política. Garantizando la identidad del suscriptor y del poseedor de la clave privada de firma, resultando idóneos para ofrecer soporte a la firma electrónica cualificada; esto es la firma electrónica avanzada basada en un certificado cualificado y generada mediante un dispositivo cualificado de creación de firma. La firma electrónica cualificada tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Asimismo, se han tenido en cuenta los estándares en materia de certificados reconocidos o cualificados, en concreto:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile (reemplaza a TS 101 862).
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

1.4.2. Usos Prohibidos y no Autorizados

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.

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 cifrado de información usando las claves asociadas al certificado

1.5. Administración de la política

1.5.1. Organización responsable:

Autoridad de certificación de la Abogacía.

Consejo General de la Abogacía Española

1.5.2. Persona de contacto:

Departamento Jurídico del Consejo General de la Abogacía Española

E-mail:	info@acabogacia.org
Teléfono:	915 23 25 93
Fax	915327836
Dirección:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

1.5.3. Responsable de la adecuación de las Prácticas y Políticas de certificación

El Consejo General de la Abogacía Española será el responsable de la correcta adecuación de las Políticas y Prácticas de Certificación

1.5.4. Procedimientos de aprobación de la Política

La publicación de las revisiones de esta Política de Certificación (CPS) deberá ser aprobada por AC Abogacía, después de comprobar el cumplimiento de los requisitos establecidos por el Consejo General de la Abogacía Española

1.6. Definiciones y Acrónimos

AC	Autoridad de Certificación, también puede encontrarse identificada por el acrónico CA (*Certification Authority*)
ACA	Autoridad de Certificación de la Abogacía
AR	Autoridad de Registro también puede encontrarse identificada por el acrónico RA (*Registration Authority*)
ARL	*Authority Revocation List*, lista de certificados revocados de la Autoridad de Certificación Raíz
CGAE	Consejo General de la Abogacía Española
CPS	*Certification Practice Statement*, Declaración de Practicas de Certificación. también puede encontrarse identificada por el acrónico DPC
CRL	*Certificate revocation list*, Lista de certificados revocados
CSR	*Certificate Signing request*, petición de firma de certificado
DES	*Data Encryption Estándar*. Estándar de cifrado de datos
DN	*Distinguished Name*, nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm*. Estándar de algoritmo de firma
DSCF/ **DCCFE**	Dispositivo Seguro de Creación de Firma Dispositivo Cualificado de Creación de Firmas Electrónicas
eIDAS	Reglamento (UE) Nº 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	*Federal information Processing Estandar publication*
IETF	*Internet Engineering task force*
ICA	Ilustre Colegio de Abogados
ISO	*International Organisation for Standardization*. Organismo intenacional de estandarización

ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones.
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso directorio
OCSP	*On-line Certificate Status Protocol*. Protocolo de acceso al estado del Certificado
OID	*Object identifier*. Identicador de Objeto
PA	*Policy Authority*. Autoridad de la Politica
PC	Política de Certificación puede encontrarse identificada por el acrónico CP (Certification Policy)
PIN	*Personal Identification Number*, Número de identificación personal
PKI	*Public Key Infrastructure*, Infraestructura de clave pública
PUK	*Personal Unblocking Key*, Código de desbloqueo
RSA	*Rivest-Shimar-Adleman*. Tipo de algoritmo de cifrado
SHA-2	*Secure Hash Algorithm*. Algoritmo seguro de Hash
TLS	*Transport Layer Security. Su antecessor es SSL (Secure Socket Layer es un p*rotocolo 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	*Transmission Control Protocol/Internet Protocol* 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 direccional adecuadamente la información hacia su destinatario

2. Cláusulas Generales Publicación y Repositorio de certificados

2.1. Repositorios

AC Abogacía podrá a disposición de los usuarios la siguiente información

- Las Prácticas y Politicas de certificación en la web www.acabogacia.org/doc
- Los términos y condiciones del servicio.
- Certificados emitidos
- Certificados de las Autoridades de Certificación
- Certificados revocados e información sobre la validez de los certificados
- El documento "PKI Disclosure Statement"(PDS) en el siguiente sitio de Internet http://www.acabogacia.org/doc/EN

2.2. Repositorio de certificados

Se podrá acceder a los certificados emitidos, siempre que el suscriptor dé su consentimiento para que su certificado sea accesible, en el sitio de Internet http://www.acabogacia.org.

Se mantendrá un repositorio de todos los Certificados emitidos, durante el periodo de vigencia de la entidad emisora

2.3. 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.

2.4. 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 desde la direcciones URL contenidas en los propios certificado en la extensión "*CRL Distribution Point*".

3. Identificación y Autenticación

3.1. Gestión de nombres

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 contendrá como mínimo 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
- Un componente de código identificativo del Autorizante con OID 1.3.6.1.4.1.16533.30.2
- Un componente de código identificativo de la AR con OID 1.3.6.1.4.1.16533.30.3.

Certificados Cualificados de Autorizado

- El valor autenticado del componente Nombre (Common Name) –CN contendrá el nombre (Nombre y Apellidos) y número de NIF 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 de la institución en la cual el suscriptor ha realizado el registro, es decir el Colegio o Consejo de Abogados.
- El valor autenticado del componente Unidad en la Organización –OU contendrá el nombre o denominación social del Autorizante.
- El valor autenticado del componente Título-T contendrá el rol del suscriptor con el valor único “Autorizado”
- 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 del suscriptor o identificador conforme ETSI EN 319 412-1.Adicionalmente, se incluirá un componente NIF/CIF, representado por el siguiente OID 1.3.6.1.4.1.16533.30.2.2), que contendrá el NIF/CIF correspondiente al Autorizante.
- 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.

El valor del componente con OID 1.3.6.1.4.1.16533.30.3 contendrá el código numérico de la Autoridad de Registro definida en el campo O. Estará compuesto por un código correspondiente una codificación interna de ACA, una barra de separación”/” y el código del Test de Compatibilidad EJIS del Consejo General del Poder Judicial si hubiese.

3.1.2. Significado de los nombre

Los nombres incluidos en los certificados serán significativos y comprensibles,

3.1.3. Pseudónimos

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

3.1.4. 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.

3.1.5. 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 y/o el NIF se usarán para distinguir entre dos identidades cuando exista algún problema sobre duplicidad 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

La AC no asumirá compromisos en la emisión de certificados respecto al uso por los suscriptores de una marca comercial. No se permitirá deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del suscriptor. Sin embargo la AC no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

3.2. Validación inicial de la identidad

3.2.1. 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.

La AR hace entrega (si no dispone de él) de un kit conteniendo el dispositivo cualificado de creación de firmas electrónicas. Si el dispositivo no ha sido previamente inicializado, el suscriptor inicializa en la propia AR y ante el operador el dispositivo cualificado de creación de firmas electrónicas. Durante este proceso se generan los datos de activación de del dispositivo, 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 cualificado de creación de firmas electrónicas, enviando por un canal seguro la clave pública 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.

Por tanto, el método de prueba de la posesión de la clave privada por el suscriptor será PKCS#10.

3.2.2. Autenticación de la identidad de una organización

Para realizar una correcta verificación de la identidad de una organización Autorizante para la emisión de certificados Cualificados de Autorizado, se justificará adecuadamente ante la Entidad de Registro, salvo que sea el propio Colegio o Consejo la Organización Solicitante:

- La acreditación por un medio fehaciente de la existencia de la entidad conforme a Derecho.
- La identidad de la persona física representante de la organización para la solicitud, y su vinculación con la organización

3.2.3. Autenticación de la identidad de un individuo

Para realizar una correcta verificación de la identidad del suscriptor, se exigirá la personación física del suscriptor ante la AR y la presentación del Documento Nacional de Identidad, el pasaporte español o Tarjeta de Extranjero ante un operador o personal debidamente autorizado de la Autoridad de Registro.

Adicionalmente, la AR requerirá una autorización expresa, firmada por el Autorizante para la emisión, bajo su responsabilidad, de un certificado digital al Suscriptor.

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.

De acuerdo con el artículo 7 de la Ley 6/2020, lo dispuesto en los párrafos anteriores podrá no ser exigible 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.

3.2.4. Información de suscriptor no verificada

Toda la información contenida en los certificados será verificada

3.2.5. Validación de las Autoridades de Registro

-

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS.

3.2.6. Criterios de interoperabilidad

No estipulado.

3.3. Identificación y autenticación de renovación de certificados

3.3.1. Renovación ordinaria

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.

El suscriptor podrá realizar la renovación online desde un mes antes de la caducidad siempre que los datos de identificación del suscriptor continúen siendo los mismos y el período de tiempo transcurrido desde la identificación inicial sea menor de cinco años.

3.3.2. Reemisión después de una revocación

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

3.4. Identificación y autenticación de una Solicitud de revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS)=

4. Requerimientos Operacionales del ciclo de vida del certificado

4.1. Solicitud de certificados

4.1.1. Quien puede solicitar un certificado

La solicitud de un certificado digital podrá realizarse personándose el solicitante en una Autorizada de Registro ante un operador debidamente autorizado.

4.2. Procedimiento de solicitud de certificados

Una vez recibida la solicitud del certificado y 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 cualificado de creación de firmas electrónicas de soporte de la clave privada y los dispositivos de acceso a él, si los hubiera.

Si el dispositivo no hubiere sido previamente inicializado, el suscriptor inicializa en la propia AR y ante el operador el dispositivo cualificado de creación de firmas electrónicas. 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. En ningún caso, las ARs custodiaran los datos de activación del dispositivo cualificado de creación de firmas electrónicas. 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 cualificado de creación de firmas electrónicas, enviando por un canal seguro la clave pública 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.

4.3. 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 cualificado de creación de firmas electrónicas 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, el suscriptor acepta su certificado en el dispositivo cualificado de creación de firmas electrónicas que custodia la clave privada.

4.4. Aceptación de certificados

Se considerará que un suscriptor acepta su certificado cuando descarga su certificado en el dispositivo cualificado de creación de firmas electrónicas 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.

Sin perjuicio de lo indicado en el párrafo anterior, el suscriptor dispondrá de un periodo máximo de siete días naturales para notificar a la AR cualquier defecto en los datos del certificado, o en la publicación de los datos del mismo en el Registro de Certificados.

4.5. Uso del par de claves y del certificado

4.5.1. Uso de las claves privada y el certificado por el suscritor

La clave privada será generada por el suscriptor y permanecerá en todo momento en posesión exclusiva del mismo. Esta custodiada en un dispositivos cualificados de creación de firmas electrónicas requiriéndose para su uso los datos de activación que sólo el suscriptor conoce.

La AC ni ARs no crea, almacena ni posee en ningún momento la clave privada del suscriptor, ni los datos de activación del dispositivo que la custodia.

4.5.2. Uso de la clave pública y certificado por un tercero que confía

Los terceros que confían en un certificado lo harán siempre de forma voluntaria asegurando que realizan las verificaciones oportunas que garantizan la validez del certificado en el que confían sujetos siempre a las limitaciones indicadas en la presente política.

4.6. Renovación de certificados

Los certificados no podrán renovarse.

4.7. Renovación de certificados y claves

Los certificados ni las claves podrán podrán renovarse

4.8. Modificación de certificados

No está permitida la modificación de certificados una vez emitidos

4.9. Suspensión y Revocación de certificados

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

4.10. Servicios de comprobación del estado de los certificados

La ACA pondrá a disposición la información relativa al estado de sus certificados a través de consultas en su web y el servicio de OCSP.

Se facilitará también información sobre la suspensión o revocación de los certificados 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).

4.11. Finalización de la suscripción

Se entenderá el fin de la suscripción del servicio cuando finalice el plazo de validez del certificado o cuando éste sea revocado.

4.12. Custodia y recuperación de claves

AC Abogacía no custodia ninguna clave privada de los usurarios por lo que no se podrán recuperar en ningún caso.

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

La generación de la clave de las CA's se realiza, de acuerdo con el proceso documentado de ceremonia de claves, dentro de la sala criptográfica del PSC, por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de la organización titular de la AC y del auditor externo.

La generación de la clave de las CA's delegadas se realiza en un dispositivo que cumple los requerimientos que se detallan en el FIPS 140-2, 3. y CC EAL4+

Las claves son generadas usando el algoritmo de clave pública RSA.

Las claves de las CA's tienen una longitud mínima de 4096 bits

Las claves de los suscriptores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-2 nivel 3, ITSEC High4 u otro de nivel equivalente.

Las claves de los suscriptores son generadas mediante dispositivos cualificados de creación de firmas electrónicas. El dispositivo SSCD ha sido evaluado según el Perfil de Protección - Secure Signature Creation Device Type 3, versión 1.05, de acuerdo con CC, version 3.1 révision 3, hasta un Nivel de Garantía de Evaluación EAL 4 aumentado con AVA_VAN.5. En conformidad con el apartado 1 de la medida transitoria del artículo 51 del Reglamento 910/2014 (eIDAs), los dispositivos seguros de creación de firma cuya conformidad se haya determinado con arreglo a lo dispuesto en el artículo 3, apartado 4, de la Directiva 1999/93/CE se considerarán dispositivos cualificados de creación de firma electrónica con arreglo al presente Reglamento.

El dispositivo cualificado de creación de firmas electrónicas 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 entregarán mediante un proceso que asegure la confidencialidad de los mismos ante terceros. En ningún caso, las ARs custodiaran los datos de activación del dispositivo cualificado de creación de firmas electrónicas.

Las claves de los suscriptores son generadas usando el algoritmo de clave pública RSA, con los adecuados parámetros. Las claves tienen una longitud mínima de 2048 bits.

Se empleará como SSCD tarjetas con criptoprocesador 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

6.1.2. Entrega de la clave privada al suscriptor

No hay entrega por parte de la AC de claves privadas.

6.1.3. 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

6.1.4. Entrega de la clave pública de la CA a los Usuarios

El certificado de las CAs de la cadena de certificación y su fingerprint (huella digital) estarán a disposición de los usuarios en http://www.acabogacia.org.

6.1.5. Tamaño de las claves

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

6.1.6. Parámetros de generación de la clave pública

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

6.1.7. 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 y controles de los módulos criptográficos

6.2.1. Estándares y controles de los módulos criptográficos

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

6.2.2. Control por más de una persona (n de m) sobre la clave privada

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

6.2.3. Custodia de la claves privada

En ningún caso la AC almacenará la clave privada del suscriptor ni de la CA en el modo llamado de key escrow

6.2.4. Backup de la clave privada

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

6.2.5. Archivo de la clave privada

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

6.2.6. Transferencia de la clave privada en o desde el módulo criptográfico

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

6.2.7. Almacenamiento de la clave privada en modulo criptográfico.

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

6.2.8. Método de activación de la clave privada

Las claves de la CA se activan por un proceso de m de n.

La clave privada del suscriptor se activa mediante la introducción del PIN en el dispositivo seguro de creación de firma.

La clave privada del suscriptor se mantendrá en un dispositivo cualificado de creación de firmas electrónicas 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.

6.2.9. Método de desactivación de la clave privada

Para certificados de firma electrónica cualificada, mediante el cierre de sesión del CPS o PKCS#11. Esto se producirá al retirar la tarjeta del lector o cuando la aplicación la cierre.

6.2.10. Método de destrucción de la clave privada

La clave privada de la CA según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

La clave privada de la CA se destruye en el proceso de renovación del certificado o bien por destrucción física del dispositivo criptográfico.

6.2.11. Evaluación del módulo criptográfico

No estipulado.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

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

6.3.2. Periodo de uso para las claves públicas y privadas

Determinado por el periodo de validez del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

El dispositivo cualificado de creación de firmas electrónicas utiliza una clave de activación para el acceso a las claves privadas.

Los dispositivos seguros de creación de firma (tarjeta) llevan incorporado de fábrica un sistema de activación de clave mediante PIN de transporte que debe ser modificado por el suscriptor en el momento de la entrega física de la tarjeta.

6.4.2. Protección de datos de activación

En caso de que la entrega del dispositivo no se realice de manera presencial en la AR, los datos de activación se entregarán mediante un proceso que asegure la confidencialidad de los mismos ante

terceros. En ningún caso, las ARs custodiaran los datos de activación del dispositivo cualificado de creación de firmas electrónicas.

6.4.3. Otros aspectos de los datos de activación

Sin especificar

6.5. Controles de seguridad informática

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

6.5.1. Requerimientos técnicos de seguridad informática específicos

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

6.5.2. Valoración de la seguridad informática

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

6.6. Ciclo de vida de los dispositivos criptográficos

6.6.1. Controles de desarrollo del sistema

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

6.6.2. Evaluación del nivel de seguridad del ciclo de vida

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

6.6.3. Evaluación del nivel de seguridad del ciclo de vida

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

6.7. Controles de seguridad de la red

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

6.8. Sellado de tiempo

No estipulado

7. Perfiles de Certificado, CRL y OCSP

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 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 firma electrónica;

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 firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;

d) datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;

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 de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

7.1.1. Número de versión

X509 Versión V3

7.1.2. Extensiones del certificado

7.1.2.1. Campos

Los certificados seguirán el estándar X509, definido en la RFC 5280 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	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)
Valido hasta (notAfter)	(fecha de fin de validez, tiempo UTC)
Asunto (Subject)	(Según especificaciones de la sección **3.1.1**)
Clave pública	RSA (2048 bits)

7.1.2.2. **Extensiones**

Se incluirán las siguientes extensiones:

EXTENSIONES	VALOR
Nombre alternativo del sujeto (SubjectAlternativeName)	Opcional
Restricciones básicas	Tipo de asunto= Entidad final

(BasicConstraints)	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: Dirección URL=http://www.acabogacia.org/certificados/aca_ca2.crt
Directivas de certificado (Certificate Policies)	Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.20.4.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc
Declaración de Certificados Calificados qcStatements x.509v3 certificate extension from RFC 3039	1.- id-etsi-qcs-QcCompliance 2.- id-etsi-qcs-QcSSCD 3.- id-etsi-qcs-QcPDS URL=http://www.acabogacia.org/doc/EN

Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/aca_ca2.crl http://crl.acabogacia.org/crl/aca_ca2.crl
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos, 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. Formato de los nombres

No estipulado.

7.1.5. Identificador de objeto de política de certificado

Según el OID indicado en el apartado 1.2

7.1.6. Empleo de la extensión restricciones de política

No está definida

7.1.7. Sintaxis y semántica de los calificadores de política

La extensión “Certificate Policies” incluye.

- Policy que contiene el OID de la política
- CPS que contiene una URL al repositorio de póliticas y CPS

7.1.8. Tratamiento semántico para la extensión “Certificate policy”

La extensión “Certificate Policy” incluye el campo OID de política, que identifica la política asociada al Certificado por parte de ACA

7.2. Perfil de CRL

7.2.1. Número de versión

Las CRLs emitidas por la AC son conformes al estándar X.509 versión 2.

7.2.2. CRL y extensiones

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

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

Se incluirán las siguientes extensiones

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

7.3. Perfil de OCSP

7.3.1. Número de versión

Los Certificados utilizados por el Servicio de información y consulta sobre el estado de validez de los certificados, vía OCSP, son conformes con el estándar X.509 versión 3.

7.3.2. Extensiones del OCSP

Las respuestas OCSP del Servicio de información y consulta sobre el estado de validez de los certificados incluyen, para las peticiones que lo soliciten, la extensión global “nonce”, que se utiliza para vincular una petición con una respuesta, de forma que se puedan prevenir ataques de repetición.

8. Auditorias de conformidad

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

9. Otros temas legales y Operativos

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

.

ANEXO 1: Información técnica

, En cumplimiento de lo establecido en el Reglamento 910/2014 y la Ley 6/2020 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 cualificado, el suscriptor deberá disponer del correspondiente dispositivo de generación de datos de creación de firmas y de creación de firmas.

A. Dispositivos Cualificado de Creación de Firma Electrónica:

Los Certificados Cualificados identificados por el OID de Política 1.3.6.1.4.16533.10.3.1 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 Anexo II de eIDAS, y que se denominan “Dispositivos Cualificados de Creación de Firmas Electrónica (DCCFE)”.

La firma electrónica avanzada generada con tales dispositivos, y basada en un certificado cualificado, se denomina “Firma Electrónica Cualificada. La firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.

La AC considera adecuados los dispositivos que cumplan lo siguiente:

Que dispongan de la correspondiente certificación de dispositivo según lo establecido en el artículo 51 de eIDAS, 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 2048 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); Cryptographic Suites” ETSI TS 119 312 y “Electronic Signatures and Infrastructures (ESI);

Guidance on the use of standards for cryptographic suites” ETSI TR 119 300 (www.etsi.org)

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 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.

- 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 subministrada 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.

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 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.