



ACA

**AUTORIDAD
DE CERTIFICACIÓN
DE LA ABOGACÍA**

Certificados cualificados de Persona Física

Política de Certificación (CP6_ACA1_002)

OID: 1.3.6.1.4.1.16533.50.6.2 QSCD centralizado

OID: 1.3.6.1.4.1.16533.50.6.3 Software

CONTROL DE VERSIONES

Versión	Fecha	Descripción / Cambios Relevantes
1.0	7/10/24	Primera versión
2.3	22/10/2025	Se elimina la Jerarquía ACA ROOT Adecuación al Reglamento (UE) 2024/1183 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 11 de abril de 2024 por el que se modifica el Reglamento (UE) n.o 910/2014. Se incluye el perfil de certificado en QSCD Centralizado

ÍNDICE

1. INTRODUCCIÓN	7
1.1. Resumen.....	7
1.2. Identificación del documento	9
1.3. Comunidad y Ámbito de Aplicación.	9
1.3.1. Autoridad de Certificación (AC).....	9
1.3.2. Autoridad de Registro (AR).....	9
1.3.3. Suscriptor.....	10
1.3.4. Usuario	10
1.3.5. Otros participantes.....	10
1.4. Ámbito de Aplicación y Usos	10
1.4.1. Usos permitidos de los certificados.....	10
1.4.2. Usos Prohibidos y no Autorizados	11
1.5. Administración de la política	12
1.5.1. Organización responsable:	12
1.5.2. Persona de contacto:.....	12
1.5.3. Responsable de la adecuación de las Prácticas y Políticas de certificación	12
1.5.4. Procedimientos de aprobación de la Política	12
1.6. Definiciones y Acrónimos	13
2. Publicación y Repositorio de Certificados	15
3. Identificación y Autenticación	16
3.1. Gestión de nombres	16
3.1.1. Tipos de nombres	16
3.1.2. Pseudónimos	17
3.1.3. Reglas utilizadas para interpretar varios formatos de nombres	17
3.1.4. Unicidad de los nombres.....	17
3.1.5. Reconocimiento, autenticación y función de las marcas registradas	17
3.2. Validación inicial de la identidad.....	17
3.2.1. Métodos de prueba de la posesión de la clave privada	17
3.2.2. Autenticación de la identidad de una organización	17
3.2.3. Autenticación de la identidad de un individuo	17
3.2.4. Información de suscriptor no verificada	18

3.2.5.	Validación de las Autoridades de Registro	18
3.2.6.	Criterios de interoperabilidad	18
3.3.	Identificación y autenticación de renovación de certificados.....	18
3.3.1.	Renovación ordinaria	18
3.3.2.	Reemisión después de una revocación	18
3.4.	Identificación y autenticación de una solicitud de revocación	18
4.	Requerimientos Operacionales del ciclo de vida del certificado	19
4.1.	Solicitud de certificados	19
4.1.1.	Quien puede solicitar un certificado	19
4.2.	Tramitación de solicitud de certificados	19
4.3.	Emisión de certificados	19
4.3.1.	Actuaciones de la AC durante la emisión de los certificados	20
4.3.2.	Notificación al suscriptor por parte de la CA de la emisión del certificado	20
4.4.	Aceptación de certificados	20
4.4.1.	Forma en la que se acepta el certificado.....	20
4.4.2.	Publicación del certificado por la AC.....	21
4.4.3.	Notificación de la emisión del certificado por la AC a otras Autoridades	21
4.5.	Uso del par de claves y del certificado	21
4.5.1.	Uso de las claves privada y el certificado por el suscriptor	21
4.5.2.	Uso de la clave pública y certificado por un tercero que confía	21
4.6.	Renovación de certificados	21
4.7.	Renovación de certificados y claves	21
4.7.1.	Circunstancias para la renovación de certificados	21
4.7.2.	Quién puede solicitar la renovación de certificados	22
4.7.3.	Tramitación de las peticiones de renovación.....	22
4.7.4.	Notificación de la renovación de certificado.....	22
4.7.5.	Aceptación de la renovación	22
4.7.6.	Publicación de la renovación de certificados	22
4.7.7.	Notificación de la renovación a otras entidades.....	22
4.8.	Modificación de certificados	23
4.9.	Suspensión y Revocación de certificados.....	23
4.10.	Servicios de comprobación del estado de los certificados.....	23

4.11.	Finalización de la suscripción	23
4.12.	Custodia y recuperación de claves	23
5.	Controles de Seguridad Física, Procedimental y de Personal	24
6.	Controles de Seguridad Técnica	25
6.1.	Generación e instalación del par de claves	25
6.1.1.	Generación del par de claves	25
6.1.2.	Entrega de la clave privada al suscriptor	25
6.1.3.	Entrega de la clave pública al emisor del certificado	25
6.1.4.	Entrega de la clave pública de la CA a los Usuarios.....	26
6.1.5.	Tamaño de las claves.....	26
6.1.6.	Parámetros de generación de la clave pública.....	26
6.1.7.	Fines del uso de la clave	26
6.2.	Protección de la clave privada y controles de los módulos criptográficos	26
6.2.1.	Estándares y controles de los módulos criptográficos.....	26
6.2.2.	Control por más de una persona (n de m) sobre la clave privada	26
6.2.3.	Custodia de la clave privada	27
6.2.4.	Backup de la clave privada	27
6.2.5.	Archivo de la clave privada.....	27
6.2.6.	Transferencia de la clave privada en o desde el módulo criptográfico.....	27
6.2.7.	Almacenamiento de la clave privada en módulo criptográfico.....	27
6.2.8.	Método de activación de la clave privada.....	27
6.2.9.	Método de desactivación de la clave privada	27
6.2.10.	Método de destrucción de la clave privada	27
6.2.11.	Evaluación del módulo criptográfico.....	28
6.3.	Otros aspectos de gestión del par de claves	28
6.3.1.	Archivo de la clave pública	28
6.3.2.	Periodo de uso para las claves públicas y privadas	28
6.4.	Datos de activación	28
6.5.	Controles de seguridad informática	28
6.6.	Controles de seguridad del ciclo de vida.....	28
6.7.	Controles de seguridad de la red	28
6.8.	Sellado de tiempo.....	28

7.	Perfiles de Certificado, CRL y OCSP	29
7.1.	Perfil de Certificado.....	29
7.1.1.	Número de versión.....	30
7.1.2.	Extensiones del certificado.....	30
7.1.3.	Identificadores de objeto (OID) de los algoritmos	35
7.1.4.	Formato de los nombres	35
7.1.5.	Restricciones de nombre.....	36
7.1.6.	Identificador de objeto de política de certificado.....	36
7.1.7.	Empleo de la extensión restricciones de política	36
7.1.8.	Sintaxis y semántica de los calificadores de política	36
7.1.9.	Tratamiento semántico para la extensión “Certificate policy”	36
7.2.	Perfil de CRL.....	36
7.2.1.	Número de versión.....	36
7.2.2.	CRL y extensiones	36
7.3.	Perfil de OCSP.....	37
7.3.1.	Número de versión.....	37
7.3.2.	Extensiones del OCSP	37
8.	Auditorias de conformidad.....	38
9.	Otros temas legales y Operativos.....	39
	ANEXO 1: Información técnica	40

1. INTRODUCCIÓN

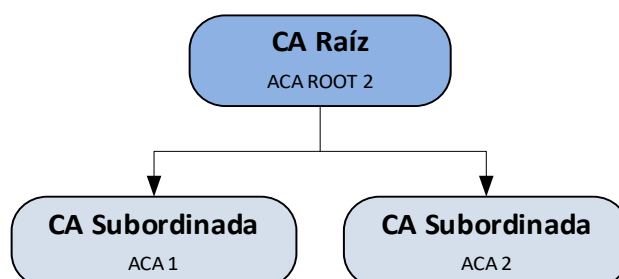
1.1. Resumen

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, modificado por el Reglamento (UE) 1183/2024 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante eIDAS).

En 2024 se han generado una nueva CA Raíz y CAs subordinadas en conformidad con la legislación vigente y se mantienen las descritas puesto que se encuentran en vigor los certificados expedidos por estas jerarquías teniendo una política de certificación propia. Los certificados definidos en esta política se expedirán mediante las nuevas CAs subordinadas.

Nueva Jerarquía 2024, compuesta de dos niveles;



El presente documento especifica la Política de Certificación del Certificado digital denominado “Certificado Cualificado de Persona Física en software” y “Certificado Cualificado de Persona Física QSCD centralizado” emitidos 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 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, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que

respecta al establecimiento del Marco Europeo de Identidad Digital (eIDAS), 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.

La Política de Certificación (en adelante PC) se ha estructurado conforme al documento RFC-3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC-3647. Cuando no se haya previsto nada en alguna sección o esta venga referida en la DPC, no se contemplará dicho apartado. Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta estándares europeos, entre los que cabe destacar los siguientes:

- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- ETSI EN 319 411-1: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 401: Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Se han tenido en cuenta los estándares en materia de certificados cualificados, en concreto:

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

En esta PC se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (DPC) del Prestador de Servicios de Confianza, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados. Todas las partes involucradas tienen la obligación de conocer la PC y ajustar su actividad a lo dispuesto en la misma.

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:	CP6_ACA1_002
O.I.D.	1.3.6.1.4.1.16533.50.6.2 QSCD Centralizado 1.3.6.1.4.1.16533.50.6.3 Software
Descripción:	Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: certificados cualificados de Persona Física
Versión:	002.3
Fecha de Emisión:	22/10/2025
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 electrónico.

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:

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

1.3.3. Suscriptor

Bajo esta Política el Suscriptor es una persona física, poseedor de un “Certificado Cualificado de Persona Física” alojado o en software. El suscriptor recibe también el nombre de “Firmante”, según se define en el art. 3.9 del Reglamento eIDAS.

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 certificados

Los certificados emitidos bajo la presente Política, permiten identificar a una persona física a título personal. Los certificados de Persona Física 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 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 íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado 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 descritos en esta política son certificados cualificados, que además son conformes con lo establecido en el artículo 28 del eIDAS.

El reglamento eIDAS establece que los Certificados Cualificados de Firma Electrónica cumplirán los requisitos establecidos en el anexo I y II. Por otro lado, la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica donde se presumirá el cumplimiento de los requisitos establecidos en dicho anexo cuando un certificado cualificado de firma electrónica se ajuste a dichas normas.

Los certificados en QSCD definidos en esta política, ya sea en tarjeta o centralizado, sirven de base para la generación de firmas electrónicas cualificadas creadas mediante un dispositivo cualificado de creación de firmas electrónicas, garantizándose las condiciones del artículo 29 y requisitos de los anexos I y II del Reglamento eIDAS.

Los certificados de Persona Física en QSCD, 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 un efecto jurídico equivalente al de una firma manuscrita.

Los certificados cualificados de Persona Física en software están indicados para soportar firma electrónica avanzada con certificados cualificados, tal y como está definido en los artículos 26 y 27 de eIDAS.

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

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

Además, estos certificados serán utilizados por los firmantes en las relaciones que mantengan con terceros que confían, de acuerdo con los usos autorizados en las extensiones “Key Usage” y “Extended Key Usage” del certificado y en conformidad con las limitaciones que consten en el 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 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 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 Practicas de Certificación. también puede encontrarse identificada por el acrónimo DPC
CRL	<i>Certificate revocation list</i> , Lista de certificados revocados
CSR	<i>Certificate Signing request</i> , petición de firma de certificado
DES	<i>Data Encryption Estándar</i> . Estándar de cifrado de datos
DN	<i>Distinguished Name</i> , nombre distintivo dentro del certificado digital
DSA	<i>Digital Signature Algorithm</i> . Estándar de algoritmo de firma
DSCF/	Dispositivo Seguro de Creación de Firma
DCCFE	Dispositivo Cualificado de Creación de Firmas Electrónicas
eIDAS	Reglamento (UE) 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 y por la que se deroga la Directiva 999/93/CE, modificado por el Reglamento (UE) 1183/2024 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital.
FIPS	<i>Federal information Processing Estandar publication</i>
QSCD	<i>Dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II de eIDAS.</i> Qualified electronic Signature/Seal Creation Device
IETF	<i>Internet Engineering task force</i>
ICA	Ilustre Colegio de Abogados
ISO	<i>International Organisation for Standardization</i> . Organismo intenacional 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 (Certification Policy)
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-Shimam-Adleman</i> . Tipo de algoritmo de cifrado
SHA-2	<i>Secure Hash Algorithm</i> . Algoritmo seguro de Hash
TLS	<i>Transport Layer Security</i> . Su antecesor es SSL (<i>Secure Socket Layer</i> es un 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

2. Publicación y Repositorio de Certificados

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

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 de Persona Física 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 Nombre de Pila (Given name)- G
- Un componente Apellido 1 “Surname” – SN
- Un componente Número de Serie –serialNumber
- Un componente E-mail –E
- Un componente Estado (Country)-C

Certificados de Persona Física

- El valor autenticado del componente Nombre (Common Name) –CN contendrá el nombre y apellidos del suscriptor.
 - o Para los certificados en software
 - Contendrá la cadena (SW)
 - CN = Nombre Apellido1 Apellido2 (SW)
 - o Para los certificados de QSCD centralizados, las opciones son las siguientes:
 - CN = Nombre Apellido1 Apellido2 (FIRMA)
 - CN = Nombre Apellido1 Apellido2 (AUTENTICACION)
- 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 Número de Serie –serialNumber contendrá el NIF del suscriptor o identificador conforme ETSI EN 319 412-1 y RFC 3739 apartado 3.2.6.1, relativo a la codificación de la información semántica. Ejemplo IDCES-11111111H.
- El valor autenticado del componente E-mail –E contendrá la dirección de correo electrónico del suscriptor.
- El valor autenticado del componente Estado (Country)-C contendrá “ES”.

3.1.2. Pseudónimos

Los certificados de persona física no admiten pseudónimos.

3.1.3. Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.4. Unicidad de los nombres

Los nombres distinguidos de los certificados emitidos serán únicos para cada suscriptor. La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres de los certificados emitidos. El atributo 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.

3.1.5. Reconocimiento, autenticación y función de las marcas registradas

No estipulado

3.2. Validación inicial de la identidad

3.2.1. Métodos de prueba de la posesión de la clave privada

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

3.2.2. Autenticación de la identidad de una organización

No aplicable a este tipo de certificados

3.2.3. 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, Tarjeta de Extranjero o medio admitido a derecho, 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.

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. 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 al menos 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 sea menor de cinco años.

En caso contrario, para renovar su certificado, el suscriptor tendrá que personarse en la Autoridad de Registro para la emisión de un nuevo certificado.

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). Consulte <http://www.acabogacia.org/doc>.

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 por una persona física mayor de edad, con capacidad plena de obrar y con capacidad jurídica suficiente, personándose ante un operador debidamente autorizado.

4.2. Tramitación 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 cuando es requerido, 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 firma del instrumento jurídico vinculante conlleva la aceptación los requisitos establecidos en la DPC y en esta PC.

En el ámbito de los certificados cualificados de Persona Física en software, tras la firma del instrumento jurídico vinculante, la Autoridad de Registro remitirá la solicitud a la Autoridad de Certificación de Abogacía de confianza para su tramitación.

Toda evidencia recogida durante el proceso quedará vinculada al mismo y custodiada por la Autoridad de Certificación de la Abogacía.

4.3. Emisión de certificados

Previo a la generación de claves y certificados, es necesaria la validación, revisión y aprobación por la AR de la solicitud de certificado, y dados de alta los datos dentro del sistema de AC Abogacía.

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

- La AR recibe la petición de emisión del certificado.
- La AR verificará la identidad del solicitante, la integridad y los datos que se incluyan en el certificado.
- En el ámbito de los certificados cualificados QCSD centralizado o en software, el proceso de emisión se realiza en los siguientes pasos
 - La AR la valida, revisa y aprueba la solicitud de certificado y los datos dados de alta dentro del sistema.
 - En una primera emisión, se envía por parte de AR de un correo electrónico al suscriptor de forma segura, con los pasos a seguir para completar el proceso y un enlace de acceso a la zona de usuario desde donde se realizará la emisión del certificado.

- El solicitante accede a la web del proceso de emisión utilizando controles y datos de contraste para verificar los datos del suscriptor siempre acompañados de un código de activación y/o un segundo factor de autenticación.
- Una vez que el usuario ha sido registrado en el sistema con nivel avanzado de garantía de registro y ha accedido, solicita expresamente la emisión de sus certificados. Dicha emisión se lleva a cabo cuando el suscriptor acceda al procedimiento de generación.
- El suscriptor deberá introducir la contraseña de protección de su clave privada, sólo conocida por él y no almacenada en los sistemas, de modo que se garantice el uso de las claves bajo su control exclusivo.
- El sistema generará su clave privada, la cual permanecerá almacenada en el dispositivo de forma protegida, de modo que se garantice su uso bajo el control exclusivo del suscriptor.
 - Las claves para los certificados cualificados de Persona Física QSCD centralizado, se generan en el dispositivo cualificado de creación de firma electrónica.
 - Para los certificados cualificados de Persona Física software, la generación de la clave, se realizará en software.
- En la finalización del proceso de emisión del Certificado cualificado, se informa al suscriptor que se encuentra disponible dicho certificado para su uso.

4.3.1. Actuaciones de la AC durante la emisión de los certificados

En la emisión de los certificados la AC:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada;
- Protege la confidencialidad e integridad de los datos de registro;
- Incluye en el certificado las informaciones establecidas en el artículo 6 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado

En la finalización del proceso de emisión del Certificado cualificado, se informa al suscriptor que se encuentra disponible dicho certificado para su uso.

4.4. Aceptación de certificados

4.4.1. Forma en la que se acepta el certificado

La aceptación del certificado es la acción mediante la cual el suscriptor da inicio a sus obligaciones respecto a la Autoridad de Certificación de la Abogacía. El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el firmante y ACA haya sido firmado o confirmado electrónicamente y los medios que permitan hacer uso del certificado se encuentren en posesión del suscriptor.

En el proceso de generación del certificado sobre un dispositivo de creación de firma centralizado o en software, el propio acto de emisión conlleva la aceptación implícita del certificado.

Como evidencia de la aceptación deberá quedar firmado el documento de conformidad por ambas partes, o la confirmación electrónica de la aceptación del mismo cuando se den las circunstancias del artículo 7.6 de la ley 6/2020.

4.4.2. Publicación del certificado por la AC

Los certificados no se publicarán en ningún repositorio de acceso libre.

4.4.3. Notificación de la emisión del certificado por la AC a otras Autoridades

No se efectúan notificaciones a terceros

4.5. Uso del par de claves y del certificado

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

El suscriptor sólo puede utilizar la clave privada y el certificado tras aceptar las condiciones de uso establecidas en la DPC y PC, el documento de aceptación medios y para los usos autorizados de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado.

El suscriptor dejará de usar la clave privada tras la expiración o revocación del certificado.

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 utilizando los medios que se establecen en la DPC y en esta PC, sujetos siempre a las limitaciones indicadas en la presente política y de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado.

4.6. Renovación de certificados

Todas las renovaciones de certificados realizadas en el ámbito de esta PC se realizarán con cambio de claves.

4.7. Renovación de certificados y claves

4.7.1. Circunstancias para la renovación de certificados

La renovación de certificados se realizará de forma online siempre y cuando los datos contenidos en el certificado sigan siendo válidos, por olvido de contraseña establecida en la emisión del certificado o por renovación si se cumplen los plazos establecidos en el art. 7.6 de la Ley 6/2020 y todavía se encuentre en vigor. En caso de cambios en los datos, formato, expiración del certificado o compromiso de claves se emitirá uno nuevo por un Operador de AR.

Toda renovación implicará la generación de nuevas claves de suscriptor.

4.7.2. Quién puede solicitar la renovación de certificados

La renovación puede ser solicitada por el propio suscriptor del certificado siempre que cuente con un certificado en vigor, no haya cambiado ningún dato del certificado y se cumplan los plazos establecidos en el art. 7.6 de la Ley 6/2020.

En caso contrario, para renovar su certificado, el suscriptor tendrá que personarse ante por un Operador de AR.

El suscriptor del certificado accede al procedimiento online de renovación y firmará la solicitud de renovación de su certificado iniciándose en ese momento la generación de uno nuevo con los mismos datos.

El suscriptor podrá iniciar el proceso de renovación de certificados de manera telemática una vez efectuados los pasos técnicos que el sistema provee para la renovación.

4.7.3. Tramitación de las peticiones de renovación

De forma automatizada, la AC informará al suscriptor de que su certificado está próximo a expirar. Para la renovación del mismo, pueden darse dos casos:

- Si ha pasado un periodo inferior a cinco (5) años desde que el firmante se personó en la AR, éste deberá efectuar el proceso de emisión de certificados sin la necesidad de la personación en la AR.
- Si ha pasado un periodo superior a cinco (5) años desde que el suscriptor se personó en la AR, éste deberá personarse nuevamente en la AR y efectuar el proceso de emisión de certificados, como si del proceso inicial se tratara.

4.7.4. Notificación de la renovación de certificado

Una vez finalizado el proceso de renovación, el usuario será informado de la correcta renovación del certificado.

Será informando también cuando el anterior certificado haya sido revocado, quedando sin efecto.

4.7.5. Aceptación de la renovación

Para el ámbito de certificados cualificados de Persona Física QSCD centralizados y en software, en la renovación del certificado, el propio acto de renovación conlleva la aceptación implícita del certificado previa aceptación y firma del documento de conformidad con la emisión del certificado cualificado confirmando electrónicamente la aceptación del mismo.

4.7.6. Publicación de la renovación de certificados

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

4.7.7. Notificación de la renovación a otras entidades

No estipulado

4.8. Modificación de certificados

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

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

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

4.11. Finalización de la suscripción

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

4.12. Custodia y recuperación de claves

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

Para las claves de la CA, según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc>.

Las claves de los suscriptores podrán ser generadas mediante Los dispositivos cualificados de creación de firmas electrónicas.

Los dispositivos SSCD cumplen los requisitos establecidos en el Anexo II de eIDAS, y se denominan “Dispositivos cualificados de Creación de Firmas Electrónicas (DCCFE)”, Son dispositivos certificados específicamente con arreglo a los requisitos aplicables de acuerdo al artículo 30.3 del Reglamento eIDAS e incluidos en la lista de dispositivos cualificados mantenida por la Comisión Europea en cumplimiento de los artículos 30,31 y 39 del Reglamento eIDAS. Encontrándose publicados en:

<https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd>

Los dispositivos cualificados de creación de firmas electrónicas utilizan una clave de activación o PIN para el acceso a las claves privadas más un segundo factor de autenticación. Los datos de activación se entregarán mediante un proceso que asegure la confidencialidad de los mismos ante terceros.

En el caso de certificados en Software, los datos de creación de firma son generados a petición del suscriptor, una vez se ha personado, ha sido validado por la Autoridad de Registro y ha firmado el documento de conformidad con la emisión del certificado.

Cuando el solicitante acceda al servicio de generación, el sistema informará al titular de que se le va a emitir su certificado y generará en ese momento su correspondiente clave privada y la almacenará en su dispositivo, estableciendo el titular su propia contraseña que únicamente el conocerá, de modo que se garantice el control exclusivo por su parte.

Las claves de usuario son generadas usando el algoritmo de clave pública RSA, con los adecuados parámetros. Las claves tienen una longitud mínima de 3072 bits.

6.1.2. Entrega de la clave privada al suscriptor

La clave privada la genera el suscriptor mediante el proceso de emisión provisto por la Autoridad de Certificación de la Abogacía, una vez ha sido personado y validado por la AR, por medio de un proceso ajustado a la Ley.

La clave privada se genera en un dispositivo cualificado de creación de firma bajo el control exclusivo del firmante y, por lo tanto, no existe ninguna entrega de la clave privada al titular.

Cuando la generación y almacenamiento de la clave se ha realizado en software, la clave privada se encuentra en posesión del titular y con la recomendación de protegerla adecuadamente para evitar usos no deseados de la misma.

6.1.3. Entrega de la clave pública al emisor del certificado

Para los certificados finales, la clave pública a ser certificada es generada junto a la clave privada sobre el dispositivo cualificado de creación de firma electrónica o generada en software para los certificados Software.

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

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

6.1.5. Tamaño de las claves

Las claves privadas del suscriptor están basadas en el algoritmo RSA con una longitud mínima de 3072 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 la cual se califica como crítica, indicando los usos habilitados de la clave.

Asimismo, pueden establecerse limitaciones adicionales mediante la extensión “Extended Key Usage”.

Para los certificados de Persona Física software en el campo “key Usage” del certificado se ha incluido el siguiente uso:

Key Usage: nonRepudiation, DigitalSignature y Key Encipherment.

Para los certificados de Persona Física QSCD centralizado, en el campo “key Usage” de los certificados se ha incluido los siguientes usos en función del certificado (autenticación o firma):

Key Usage: nonrepudiation (para certificado de firma), DigitalSignature y Key Encipherment, (para certificado de autenticación).

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 clave privada

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

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 módulo 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

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

6.2.9. Método de desactivación de la clave privada

La desactivación se realizará cuando el firmante cierre la aplicación software de creación de firma.

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

Para las claves generadas en software es responsabilidad del titular desactivar el acceso a la clave privada.

6.2.10. Método de destrucción de la clave privada

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

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

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

6.5. Controles de seguridad informática

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

6.6. Controles 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

Los certificados emitidos bajo esta política, serán conformes con lo dispuesto en las siguientes normas y especificaciones técnicas:

- RFC 5280 “Internet X.509 Public Key Infrastructure. Certificate and CRL Profile”.
- RFC 3739 “Internet x509 Public Key Infrastructure. Qualified Certificates Profile”
- Estándar X.509 versión 3.
- Perfiles de Certificados derivados de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y al Reglamento eIDAS, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- ETSI EN 319 412-2: Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

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:

Certificados emitidos por ACA 1

CAMPOS	
Versión	V3
Nº Serie (Serial)	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)
Algoritmo de Firma	ecdsaWithSHA256
Emisor (issuer)	CN = ACA 1 O = CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA OI = VATES-Q2863006I OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA C = ES
Válido desde (notBefore)	(fecha de inicio de validez, tiempo UTC)
Válido hasta (notAfter)	(fecha de fin de validez, tiempo UTC)
Asunto (Subject)	(Según especificaciones de la sección 3.1.1)
Clave pública	RSA-3072 Bits o RSA-4096 Bits

7.1.2.2. Extensiones

Los OIDs de los atributos definidos por ACA en el sub-campo DirectoryName de la extensión SubjectAltName se describen en el cuadro siguiente:

OID	Concepto	Descripción
1.3.6.1.4.1.16533.100.1	Nombre	Nombre de pila del Suscriptor.
1.3.6.1.4.1.16533.100.2	Apellido 1	Primer apellido del Suscriptor.
1.3.6.1.4.1.16533.100.3	Apellido 2	Segundo apellido del Suscriptor.

Se incluirán las siguientes extensiones:

- Certificado Cualificado de Persona Física QSCD centralizado (Firma) emitidos por ACA 1

EXTENSIONES	VALOR
Identificador de clave del titular (SubjectKeyIdentifier)	Valor del identificador de clave del titular
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	Valor del Identificador de clave de entidad emisora
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://acaocsp.acabogacia.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://acacert.acabogacia.org/aca1_cer.crt



Nombre alternativo del titular (Subject Alternative Name)	
DirectoryName	
1.3.6.1.4.1.16533.100.1	Nombre
1.3.6.1.4.1.16533.100.2	Apellido 1
1.3.6.1.4.1.16533.100.3	Apellido 2
Directivas de certificado (Certificate Policies)	[1] Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.50.6.2 [1,1] Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc [2] Directiva de certificados: Identificador de directiva=0.4.0.194112.1.2 (qcp-natural-qscd)
Declaración de Certificados Calificados qcStatements x.509v3 certificate extension from RFC 3739	1.- id-etsi-qcs-QcCompliance 2.- QcEuRetentionPeriod: 15 años 3.- id-etsi-qcs-QcSSCD 4.- id-etsi-qcs-QcPDS URL=https://www.acabogacia.org/doc/EN 5.- QCSyntax-v2 id-etsi-qcs-SemanticsId-Natural 6.- QcType: id-etsi-qct-esign
Punto de distribución de la CRL (CRLDistributionPoint)	http://acacrl.acabogacia.org/crl/aca1_crl[N].crl https://acacrl.acabogacia.org/crl/aca1_crl[N].crl
Uso de la Clave (KeyUsage) Marcada como crítica	Sin repudio



ACA

AUTORIDAD
DE CERTIFICACIÓN
DE LA ABOGACÍAAbogacía
Española
CONSEJO GENERAL

- Certificado Cualificado de Persona Física QSCD centralizado (Autenticación) emitidos por ACA 1

EXTENSIONES	VALOR
Identificador de clave del titular (SubjectKeyIdentifier)	Valor del identificador de clave del titular
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	Valor del Identificador de clave de entidad emisora
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://acaocsp.acabogacia.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://acacert.acabogacia.org/aca1_cer.crt
Nombre alternativo del titular (Subject Alternative Name)	
DirectoryName	
1.3.6.1.4.1.16533.100.1	Nombre
1.3.6.1.4.1.16533.100.2	Apellido 1
1.3.6.1.4.1.16533.100.3	Apellido 2
Directivas de certificado (Certificate Policies)	[1] Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.50.6.2 [1,1] Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc

	[2]Directiva de certificados: Identificador de directiva=0.4.0.2042.1.2 (NCP+)
Punto de distribución de la CRL (CRLDistributionPoint)	http://acacrl.acabogacia.org/crl/aca1_crl[N].crl https://acacrl.acabogacia.org/crl/aca1_crl[N].crl
Uso de la Clave (KeyUsage) Marcada como crítica	Firma digital, Cifrado de clave

- Certificado Cualificado de Persona Física en software emitidos por ACA 1

EXTENSIONES	VALOR
Identificador de clave del titular (SubjectKeyIdentifier)	Valor del identificador de clave del titular
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	Valor del Identificador de clave de entidad emisora
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://acaocsp.acabogacia.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://acacert.acabogacia.org/aca1_cer.crt
Nombre alternativo del titular (Subject Alternative Name)	(Opcional)
DirectoryName	

1.3.6.1.4.1.16533.100.1	Nombre
1.3.6.1.4.1.16533.100.2	Apellido 1
1.3.6.1.4.1.16533.100.3	Apellido 2
Directivas de certificado (Certificate Policies)	[1] Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.50.6.3 [1,1] Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc [2] Directiva de certificados: Identificador de directiva=0.4.0.194112.1.0 (qcp-natural)
Declaración de Certificados Calificados qcStatements x.509v3 certificate extension from RFC 3739	1.- id-etsi-qcs-QcCompliance 2.- QcEuRetentionPeriod: 15 años 4.- id-etsi-qcs-QcPDS URL=https://www.acabogacia.org/doc/EN 5.- QCSyntax-v2 id-etsi-qcs-SemanticsId-Natural 6.- QcType: id-etsi-qct-esign
Punto de distribución de la CRL (CRLDistributionPoint)	http://acacrl.acabogacia.org/crl/aca1_crl[N].crl https://acacrl.acabogacia.org/crl/aca1_crl[N].crl
Uso de la Clave (KeyUsage) Marcada como crítica	Firma digital, Sin repudio, Cifrado de clave

7.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será:

- 1.2.840.10045.4.3.2 ecdsaWithSHA256

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

Los certificados contienen el “distinguished name X.500” del emisor y del titular del certificado en los campos “issuer” y “subject” respectivamente.

7.1.5. Restricciones de nombre

No se emplean restricciones de nombres.

7.1.6. Identificador de objeto de política de certificado

Según el OID indicado en el apartado 1.2

7.1.7. Empleo de la extensión restricciones de política

No está definida

7.1.8. Sintaxis y semántica de los calificadores de política

La extensión “Certificate Policies” incluye.

- Policy que contiene el OID de la política de cada tipo de certificado.
- CPS que contiene una URL al repositorio de políticas y CPS-

Y el siguiente “Policy Identifier”:

Para los certificados software:

- QCP-n (0.4.0.194112.1.0): indicación de certificado cualificado de firma, acorde a eIDAS.

Para los certificados QSCD centralizado:

- QCP-n-qscd (0.4.0.194112.1.2): indicación de certificado cualificado de firma, acorde a eIDAS. Sólo para el certificado de firma.
- NCP+ (0.4.0.2042.1.2): Indicación de certificado acorde a una política normalizada, en dispositivo seguro acorde al Reglamento eIDAS. Sólo para el certificado de autenticación.

7.1.9. 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 CRL emitidas por la AC son conformes al estándar X.509 versión 2.

7.2.2. CRL y extensiones

- Para certificados emitidos con ACA 1

[http://acacrl.acabogacia.org/crl/aca1_crl\[N\].crl](http://acacrl.acabogacia.org/crl/aca1_crl[N].crl)
[https://acacrl.acabogacia.org/crl/aca1_crl\[N\].crl](https://acacrl.acabogacia.org/crl/aca1_crl[N].crl)

Se incluirán las siguientes extensiones

Extensiones
Versión
Emisor
Fecha Inicio de Validez
Fecha Fin de Validez
Algoritmo de Firma
Algoritmo Hash de firma
Identificador de la clave de autoridad
Número de CRL
CRL incluye certificados expirados

7.3. Perfil de OCSP

El perfil del certificado de OCSP se corresponde con el estándar X.509 versión 3 de la RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - 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 son según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte <http://www.acabogacia.org/doc.>

8. Auditorias de conformidad

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

9. Otros temas legales y Operativos

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

ANEXO 1: Información técnica

En cumplimiento de lo establecido en el Reglamento eIDAS 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.

Los certificados cualificados identificados por el OID de Política 1.3.6.1.4.1.16533.50.6.2 y 1.3.6.1.4.1.16533.50.6.3, están indicados para soportar firma electrónica avanzada con certificados cualificados, tal y como está definido en los artículos 26 y 27 de eIDAS. Una firma electrónica avanzada cumplirá los requisitos siguientes:

- a) estar vinculada al firmante de manera única;
- b) permitir la identificación del firmante;
- c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
- d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable

A. Dispositivos Cualificados de Creación de Firma Electrónica:

Los Certificados cualificados identificados por el OID de Política 1.3.6.1.4.1.16533.50.6.2 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 Electrónicas (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:

Los Certificados cualificados identificados por el OID de Política 1.3.6.1.4.1.16533.50.6.3, certificados cualificados de Persona Física en Software, requieren, para su emisión que los datos de creación de firma hayan sido generados a petición del solicitante, una vez se ha personado, ha sido validado por la Autoridad de Registro y ha firmado el documento de conformidad con la emisión del certificado.

Cuando el solicitante acceda al servicio de generación, el sistema informará al titular de que se le va a emitir su certificado y generará en ese momento su correspondiente clave, estableciendo el titular su propia contraseña que únicamente el conocerá, de modo que se garantice el control exclusivo por su parte. La generación de la clave se realizará en software.

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 mínimo 3072 bits).

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 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.



ACA

AUTORIDAD
DE CERTIFICACIÓN
DE LA ABOGACÍA



Abogacía
Española
CONSEJO GENERAL

- 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.