Abogacía Española
CONSEJO GENERAL

AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

Certificados cualificados de sello eléctrónico

Política de Certificación (CP2_ACATC_009.0)

Documento Público

CONTROL DE VERSIONES

Versión	Fecha	Descripción / Cambios Relevantes
01/10/2010	CP2_ACATC_001.0	Versión inicial
01/03/2012	CP2_ACATC_002.0	Se elimina referencia a la LAECSP y a los certificados reconocidos
13/03/2014	CP2_ACATC_003.0	Se incluye una descripción de la Jerarquía PKI Se elimina detalles del modelo de módulo Criptográfico Se incrementa la longitud de las claves de usuario a 2048 bits Se indican los nuevos puntos de distribución de CRL Corrección de erratas
27/06/2016	CP2_ACATC_004.0	Se incluye nueva Jerarquía PKI, información nuevos certificados CAs Se alinea con eIDAS Adaptación de servicios reconocidos a cualificados
03/05/2017	CP2_ACATC_005.0	Se modifica el KeyUsage para alinearlo con el ETSI EN 319 412 incluyendo no repudio, firma digital y cifrado de clave Se elimina el número de serie del DN
03/05/2017	CP2_ACATC_006.0	Adecuación RFC 3647 Se referencia todo lo relativo a Otros temas Operativos y Legales (punto 9) a la CPS
02/07/2020	CP2_ACATC_007.0	Se actualiza el apartado Autenticación de la identidad de un individuo
31/05/2022	CP2_ACATC_008.0	Cambio de plantilla del documento Eliminación apartados duplicados con la CPS Adecuación legislativa Ley 6/2020, de 11 de noviembre Se indica en el apartado 3.3.1 que los certificados no se pueden renovar
21/03/2023	CP2_ACATC_009.0	Revisión legislativa anual

ÍNDICE

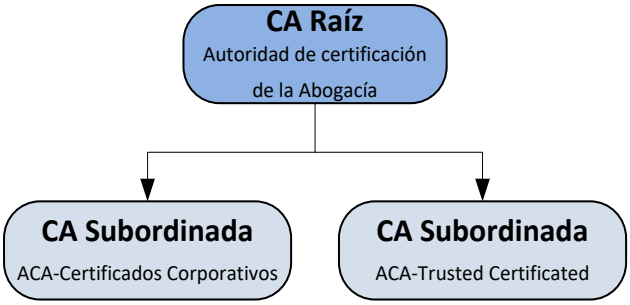
1. Introducción

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

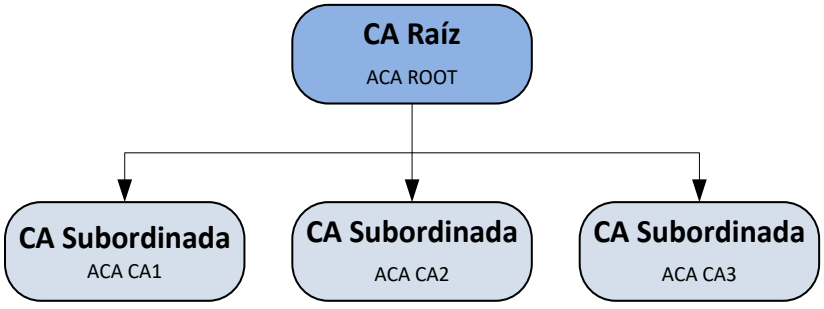


En el año 2014 se han generado nuevas CAs subordinadas con la misma denominación seguida del año de emisión: *ACA – Certificados Corporativos 2014 y ACA-Trusted Certificates 2014.*

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

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

Nueva Jerarquía 2016, compuesta de nos niveles;



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

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

Esta Política de Certificación está en conformidad con 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:	CP2_ACATC_009.0
O.I.D.	1.3.6.1.4.1.16533.20.3.1
Descripción:	Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: Certificados cualificados de sello electrónico
Versión:	009.0
Fecha de Emisión:	21/03/2023
Localización:	www.acabogacia.org/doc

CPS relacionada	
O.I.D.	1.3.6.1.4.1.16533.10.1.1

Descripción:	Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Abogacía
Localización:	www.acabogacia.org/doc

1.3. Comunidad y Ámbito de Aplicación.

1.3.1. Autoridad de Certificación (AC)

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

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

1.3.2. Autoridad de Registro (AR)

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

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

1.3.3. Suscriptor

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

1.3.4. 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 identificación y autentificación de un sistema o aplicación así como medio para autenticar los documentos electrónicos que este produzca. y en consecuencia se sujeta a lo dispuesto en esta Política, en la Declaración de Prácticas de Certificación (CPS)aplicable y la legislación vigente, por lo que no se requerirá acuerdo posterior alguno.

1.3.5. Otros participantes

No estipulado

1.4. Ámbito de Aplicación y Usos

1.4.1. Usos permitidos de los certificados

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

1.4.2. 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.

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:	Tel. 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	*Certifícate 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
ENS	Esquema Nacional de Seguridad. Adaptación de la norma ISO 27001 de la seguridad de la información al ámbito del Estado Español. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
LOPD-GDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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.509, y los atributos especificados en la recomendación ITU-T X.520 [1]

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

- Un componente Nombre (Common Name) –CN
- Un componente E-mail –E
- Un componente Organización –O
- Un componente Identificador de la Organización –OI
- Un componente Unidad en la Organización –OU
- Un componente Estado (Country)-C
- Un componente localidad- L

- El valor autenticado del componente Nombre (Common Name) –CN contendrá la denominación del sistema o aplicación de proceso automático
- El valor autenticado del componente E-mail –E contendrá la dirección de correo de contacto de la entidad suscriptora del certificado
- El valor autenticado del componente Organización –O contendrá el nombre de la organización (suscriptor del certificado)
- El valor autenticado del componente Identificador de la Organización –OI contendrá una identificación del suscriptor diferente del nombre de la organización (suscriptor del certificado). Este valor cumplirá la semántica definida en el apartado 5, de ETSI EN 319 412-1 [i.4]
- El valor autenticado del componente Unidad en la Organización –OU contendrá la naturaleza del certificado (sello electrónico para la actuación automatizada).
- El valor autenticado del componente Estado (Country)-C contendrá “ES”
- El valor autenticado del componente Localidad-L contendrá la ubicación de la sede social de la entidad suscriptora

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 sello electrónico no admiten pseudónimos.

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 de la Razón Social de la entidad, y/o el CIF darán para distinguir entre dos identidades cuando exista algún problema sobre duplicidad de nombres.

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

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

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

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

3.1.6. Reconocimiento, autenticación y función de las marcas registradas

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

3.2. Validación inicial de la identidad

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

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

3.2.2. Autenticación de la identidad de una organización

Se requerirá para todas las sociedades el Número de identificación fiscal (CIF) de la sociedad.

3.2.3. Autenticación de la identidad de un individuo

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

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

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

CSegún 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

Los certificados no podrán renovarse.

3.4. Reemisión después de una revocación

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

3.5. Identificación y autenticación de una solicitud de revocación

Pueden solicitar la suspensión o revocación de un certificado:

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

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

4. Requerimientos Operacionales del ciclo de vida del certificado

4.1. Solicitud de certificados

4.1.1. Quien puede solicitar un certificado

La AR gestiona las solicitudes de Certificados de sello electrónico

La solicitud de un certificado digital podrá realizarse personándose el solicitante en la Autoridad de registro ante un operador debidamente autorizado.

4.2. Procedimiento de solicitud de certificados

Una vez recibida la solicitud del 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.

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

4.4. Aceptación de certificados

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

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

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

4.5. 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.

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

6.1.2. Entrega de la clave 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 PKCS10 generado por el suscriptor tiene que ser transferido a la AC, de forma que se asegure que:

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

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

El certificado de las CAs de la cadena de certificación y su fingerprint 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 mínima 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/

6.2.2. 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

6.2.3. Backup de la clave privada

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

6.2.4. Archivo de la clave privada

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

6.2.5. 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

6.2.6. 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

6.2.7. 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.

6.2.8. 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.

6.2.9. 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.

6.2.10. Evaluación del módulo criptográfico

No estipulado

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 de sello electrónico incluirán, al menos, los siguientes datos:

una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de sello electrónico;

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

a. para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
b. para personas físicas, el nombre de la persona;
c. al menos, el nombre del creador del sello y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;
d. los datos de validación del sello electrónico que correspondan a los datos de creación del sello electrónico;
e. los datos relativos al inicio y final del período de validez del certificado;
f. el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;
g. la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
h. el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);

i. la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;

j. cuando los datos de creación del sello electrónico relacionados con los datos de validación del sello electrónico se encuentren en un dispositivo cualificado de creación de sellos electrónicos, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

7.1.1. Número de versión

X509 Versión V3

7.1.2. Extensiones de 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 – Trusted Certificates

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

Clave pública	RSA (1024 bits)

Certificados emitidos por ACA – Trusted Certificates 2014

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

Certificados emitidos por ACA CA2

CAMPOS	
Versión	V3
Nº Serie (Serial)	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)

Algoritmo de Firma	Sha256WithRSAEncryption
Emisor (issuer)	CN = ACA CA2 OI = VATES-Q2863006I OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA O = CONSEJO GENERAL DE LA ABOGACIA C = ES
Valido desde (notBefore)	(fecha de inicio de validez, tiempo UTC)
Válido hasta (notAfter)	(fecha de fin de validez, tiempo UTC)
Asunto (Subject)	(Según especificaciones de la sección **3.1.1**)
Clave pública	RSA (2048 bits)

7.1.2.2. Extensiones

Se incluirán las siguientes extensiones:

Certificados emitidos por ACA – Trusted Certificates

EXTENSIONES	
Nombre alternativo del emisor (IssuerAlternativeName)	Nombre RFC822=ac@acabogacia.org Dirección URL=http://www.acabogacia.org
Nombre alternativo del sujeto (SubjectAlternativeName)	Nombre RFC822=xxxx.xxxxx@cgae.es
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos
Uso mejorado de las claves (ExtendedKeyUsage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)

Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	5a f6 34 ce 96 76 56 b7 7c e9 dc dc 1d 13 6c 79 de 0f 30 76
Identificador de clave de asunto (SubjectKeyIdentifier)	
Bases de certificado (SubjectStatement)	Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.16533.20.3.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://www.acabogacia.org/doc [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario
Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/acatrusted.crl http://crl.acabogacia.org/crl/acatrusted.crl
Restricciones básicas (BasicConstraints)	Tipo de asunto= Entidad final Restricción de longitud de ruta= Ninguno
Acceso a la Información de Autoridad (Authority Information Access)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.acabogacia.org/certificados/ACAtrusted.crt
qcStatements x.509v3 certificate extension from RFC 3039	

Certificados emitidos por ACA – Trusted Certificates 2014

EXTENSIONES	
Nombre alternativo del sujeto (SubjectAlternativeName)	Opcional
Restricciones básicas (BasicConstraints)	Tipo de asunto= Entidad final Restricción de longitud de ruta= Ninguno
Identificador de clave del titular (SubjectKeyIdentifier)	
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	81 8F D1 63 00 4A CA 4D 20 97 A6 52 00 60 2E D2 CC 36 8B 6D
Uso mejorado de las claves (ExtendedKeyUsage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Acceso a la Información de Autoridad (Authority Information Access)	[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://ocsp.redabogacia.org [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.acabogacia.org/certificados/ACAtrustedV2.crt
Directivas de certificado (Certificate Policies)	Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.20.3.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS

	Certificador: http://www.acabogacia.org/doc
Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/ACAtrustedV2.crl http://crl.acabogacia.org/crl/ACAtrustedV2.crl
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos, Contrato de claves

Certificados emitidos por ACA CA2

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

	Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.acabogacia.org/certificados/aca_ca2.crt
Directivas de certificado (Certificate Policies)	Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.20.3.1 [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-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

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

Para Certificados emitidos por la CA ACA – Trusted Certificates

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

http://crl.acabogacia.org/crl/ACAtrusted.crl

Para Certificados emitidos por la CA ACA – Trusted Certificates 2014

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

http://crl.acabogacia.org/crl/ACAtrustedV2.crl

Para certificados emitidos con la ACA CA2

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

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

No estipulado.

Creación y verificación de firmas

Estándares y parámetros admitidos

No estipulado.

Métodos de verificación de firmas

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

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

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