Autoridad de Certificación de la Abogacía

Referencia: **CP1_ACA_CA3_003.0**
Fecha: **03/05/2020**
Estado del documento: **Publicado**

**Consejo General de la Abogacía Española**

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

# CP1_ACA_CA3_003.0
# CERTIFICADOS CUALIFICADOS DE AUTENTICACIÓN DE SITIO WEB

(VERSIÓN 003.0)

Control del Cambios

| Fecha | Versión | Cambios |
|---|---|---|
| 27/06/2016 | **CP1_ACA_CA3_001.0** | Versión inicial |
| 03/05/2017 | **CP1_ACA_CA3_002.0** | Se realizan las siguientes modificaciones del perfil del certificado:<br>Se incluye el qctype<br>Se incluyen nuevos campos en el subject<br>Se incluye referencia a la adhesión a CAB Forum<br>Se incluye información relativa al OCSP<br>Se incluye información acerca de la renovación y suspensión<br>Se limita la duración a 825 días<br>Se incluyen nuevas extensiones en el certificados |
| 03/05/2020 | **CP1_ACA_CA3_003.0** | Adecuación RFC 3647<br>Se referencia todo lo relativo a Otros temas Operativos y Legales ( punto 9) a la CPS<br>Se actualiza el punto 4.2 |
| | | |
| | | |
| | | |
| | | |
| | | |

# Índice de Contenido

# 1. Introducción

## *1.1. Vista General*

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

El presente documento especifica la Política de Certificación del Certificado digital denominado **"Certificado Cualificado de Autenticación de Sitios Web"** o simplemente "Certificado de SSL" emitido por la Autoridad de Certificación del Consejo General de la Abogacía Española, o AC Abogacía.

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

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

Todos los certificados emitidos bajo esta política están en conformidad con la versión actual de las Guías de CA/Browser Forum para la Emisión y Gestión de Certificados de Validación Extendida publicadas en http://www.cabforum.org. En caso de cualquier incompatibilidad entre este documento y dichos requisitos, los requisitos tienen prioridad sobre este documento.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:** | CP1_ACA_CA3_003.0 |
| **O.I.D.** | 1.3.6.1.4.1.16533.40.1.1 |
| **Descripción:** | Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: Certificados Cualificados de Autenticación de Sitios Web |
| **Versión:** | 003.0 |
| **Fecha de Emisión:** | 03/05/2020 |
| **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 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 exclusivamente el Consejo General de la Abogacía Española (CGAE)

### 1.3.3 Suscriptor

Bajo esta Política el Suscriptor es una persona jurídica tanto un Colegio de Abogados, el Consejo General de la Abogacía como un Consejo Autonómico poseedor de un "Certificado Cualificado de Autenticación de Sitios Web" y, en general, cualquier persona jurídica vinculada o relacionada de alguna forma con el Consejo General de la Abogacía Española o con los Colegios de Abogados de España.

### 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 de un sitio web así como de garantía de confidencialidad de las comunicaciones establecidas con ese sitio web y en consecuencia se sujeta a lo dispuesto en esta Política, en la Declaración de Prácticas de Certificación (CPS)aplicable y la legislación vigente, por lo que no se requerirá acuerdo posterior alguno.

### 1.3.5 Otros participantes

No estipulado

## *1.4. Ámbito de Aplicación y Usos*

### 1.4.1 Usos permitidos de los certificado

El Certificado emitido bajo la presente Política permite identificar y vincular una determinada URL a una determinada entidad, ya sea un Colegio de Abogados, el Consejo General de la Abogacía Española o un Consejo Autonómico, así como cualquier persona jurídica vinculada al ejercicio profesional de la Abogacía, permitiendo además que las sesiones entre los servidores de los dominios web y los ordenadores de los usuarios sean cifradas

El certificado emitido bajo esta Política puede ser utilizado con el siguiente propósito de la identificación de la URL. El usuario que acceda a la URL para la cual se ha emitido este certificado puede comprobar los datos de la entidad que ha registrado el dominio, demostrando la asociación de la clave privada con la clave pública asociada al certificado.

A pesar de ser posible su utilización para la autenticación de clientes en el servidor, la AC no se responsabiliza por esta actividad.

### 1.4.2 Usos Prohibidos y no Autorizados

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

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

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

La AC no se responsabiliza del contenido de las páginas Web identificadas 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<br>Paseo de Recoletos, 13<br>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<br>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.501

### 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 autenticación de sitios web no admiten seudónimos. Tampoco se pueden emplear seudónimos para identificar a una organización.

### 3.1.4 Reglas utilizadas para interpretar varios formatos de nombres

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

### 3.1.5 Unicidad de los nombres

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para garantizar que no existan dos certificados activos para la misma URL con información diferente.
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

Se podrá admitir la identificación en función de las marcas registradas.

## *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

Los certificados emitidos bajo la presente Política identifican a una entidad a cuyo nombre ha sido registrado un dominio.

La AR verificará con sus propias fuentes o fuentes externas de información los datos a incluir en el certificado.

### 3.2.3 Autenticación de la identidad de un individuo

No aplicable

### 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

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

- Que existe un contrato en vigor entre la AC y la AR, concretando los aspectos concretos de la delegación y las responsabilidades de cada agente.
- Que la identidad de la AR y de los operadores de la AR ha sido correctamente comprobada y validada.
- Que los operadores de la AR han recibido formación suficiente para el desempeño de sus funciones.
- Que la AR asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones.

- Que la comunicación entre la AR y la AC, se realiza de forma segura mediante el uso de certificados digitales.
- Que las ARs se comprometen a cumplir con los requerimientos generales de seguridad indicados por la AC.

### 3.2.6 Criterios de interoperabilidad

No estipulado

## *3.3. Identificación y autenticación de renovación de certificados*

### 3.3.1 Renovación ordinaria

La renovación de certificados consistirá en la emisión de un nuevo certificado al suscriptor a la fecha de caducidad del certificado original. Antes de renovar un certificado, la AR deberá comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor continúan siendo válidos.

Las evidencias de validación de la identidad y dominio son válidas durante un periodo máximo de 13 meses. Si la solicitud de renovación se realiza a posteriori de este tiempo será necesario realizar nuevamente todo el proceso de validación asociado a la emisión de los certificados de autenticación web.

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

### 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*

Todas las solicitudes de revocación deberán ser autenticadas

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 del suscriptor.
- Los operadores autorizados de la AC o de la jerarquía de certificación.

En cualquiera de los dos últimos casos deberán concurrir las circunstancias que se establecen en el apartado establecido por la Declaración de Prácticas de Certificación (CPS), 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

### 4.1.1 Quien puede solicitar un certificado

La solicitud de un certificado digital podrá realizarse por una persona física, autorizada ante un operador debidamente autorizado.

## *4.2. Procedimiento de solicitud de certificados*

Una vez recibida la solicitud del certificado y antes de comenzar el procedimiento de emisión, la AC deberá informar al suscriptor de los términos y condiciones relativos al uso del certificado

La AC deberá comunicar esta información a través de un medio de comunicación perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.

La AR deberá comprobar la existencia del dominio solicitado y su registro a favor de la entidad solicitante

Adicionalmente, cuando se solicite la emisión de un certificado de servidor seguro acogido a los requisitos de emisión de CA/Browser Forum, se realizará la comprobación de que el cliente ha autorizado a la Autoridad de Certificación de la Abogacía (ACA) como una CA que puede emitir certificados a su dominio. Para realizar esta comprobación, se seguirá lo estipulado en la RFC 6844 de IETF de fecha de publicación enero 2013. El cliente tiene que incluir la etiqueta de acabogacia.org en el registro CAA (Autorización de la Autoridad de Certificación en sus siglas en inglés) de su DNS. ACA realiza también las correspondientes verificaciones de que el dominio no pertenezca a dominios problemáticos o de riesgo.

## *4.3. Emisión de certificados*

La AC deberá poner todos los medios que tiene a su alcance para asegurar que la emisión de certificados se realizará de forma segura. En particular la AC deberá realizar los siguientes esfuerzos mínimos:

- La AC deberá realizar los esfuerzos razonables que estén a su alcance para confirmar la unicidad de los DN asignados
- La confidencialidad y la integridad de los datos será protegidos cuando estos sean intercambiados con el suscriptor o entre distintos componentes del sistema de certificación.
- La AC deberá verificar que el registro de los datos es intercambiado con los proveedores de servicios reconocidos, cuya identidad es autenticada

- La AC deberá notificar al solicitante la emisión del certificado.

## *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. Esta custodiada en un dispositivos cualificados de creación de firmas electrónicas requiriéndose para su uso los datos de activación que sólo el suscriptor conoce.

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

### 4.5.2 Uso de la clave 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*

No se permite la renovación automática de certificados.

## *4.7. Renovación de certificados y claves*

No se permite la renovación automática de certificados y claves.

## *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

La AC de ACA no permite la suspensión de certificados de autenticación Web.

## *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.

La AC realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de los suscriptores 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 publica 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 legitimo usuario que aparece en el certificado

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

Los certificados de las CA's de la cadena de certificación, estarán a disposición de los usuarios en http://www.acabogacia.org

### 6.1.5 Tamaño de las claves

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

### 6.1.6 Parámetros de generación de la clave pública

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

### 6.1.7 Fines del uso de la clave

La Clave privada del Suscriptor deberá se usada únicamente para la autenticación de servidor.

## *6.2. Protección de la clave privada y controles de los módulos criptográficos*

### 6.2.1 Estándares y controles de los módulos criptográficos

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

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

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

### 6.2.3 Custodia de la claves privada

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

### 6.2.4 Backup de la clave privada

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

### 6.2.5 Archivo de la clave privada

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

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

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

### 6.2.7 Almacenamiento de la clave privada en modulo criptográfico.

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

### 6.2.8 Método de activación de la clave privada

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

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

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

### 6.2.9 Método de desactivación de la clave privada

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

### 6.2.10 Método de destrucción de la clave privada

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

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

### 6.2.11 Evaluación del módulo criptográfico

No estipulado

## *6.3. Otros aspectos de gestión del par de claves*

### 6.3.1 Archivo de la clave pública

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

### 6.3.2 Periodo de uso para las claves públicas y privadas

Determinado por el periodo de validez del certificado.

## *6.4. Datos de activación*

### 6.4.1 Generación e instalación de datos de activación

El dispositivo cualificado de creación de firmas electrónicas utiliza una clave de activación para el acceso a las claves privadas.
Los dispositivos seguros de creación de firma (tarjeta) llevan incorporado de fábrica un sistema de activación de clave mediante PIN de transporte que debe ser modificado por el suscriptor en el momento de la entrega física de la tarjeta.

### 6.4.2 Protección de datos de activación

En caso de que la entrega del dispositivo no se realice de manera presencial en la AR, los datos de activación se entregarán mediante un proceso que asegure la confidencialidad de los mismos ante terceros. En ningún caso, las ARs custodiaran los datos de activación del dispositivo cualificado de creación de firmas electrónicas.

### 6.4.3 Otros aspectos de los datos de activación

Sin especificar

## *6.5. Controles de seguridad informática*

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

### 6.5.1 Requerimientos técnicos de seguridad informática específicos

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

### 6.5.2 Valoración de la seguridad informática

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

## *6.6. Ciclo de vida de los dispositivos criptográficos*

### 6.6.1 Controles de desarrollo del sistema

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

### 6.6.2 Evaluación del nivel de seguridad del ciclo de vida

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

### 6.6.3 Evaluación del nivel de seguridad del ciclo de vida

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

## *6.7. Controles de seguridad de la red*

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

## *6.8. Sellado de tiempo*

No estipulado

# 7. Perfiles de Certificado , CRL y OCSP )

## *7.1. Perfil de Certificado*

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

Los certificados cualificados de autenticación de sitios web 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 autenticación de sitio web;
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,
c) para personas jurídicas: al menos el nombre de la persona jurídica a la que se expida el certificado y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;
d) elementos de la dirección, incluida al menos la ciudad y el Estado, de la persona física o jurídica a quien se expida el certificado, y, cuando proceda, según figure en los registros oficiales;
e) el nombre o los nombres de dominio explotados por la persona física o jurídica a la que se expida el certificado;
f) los datos relativos al inicio y final del período de validez del certificado;
g) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;
h) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
i) 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 h);
j) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;

### 7.1.1 Número de versión

X509 Versión V3

### 7.1.2 Extensiones del certificado

#### 7.1.2.1 Campos

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

| **CAMPOS** | |
|---|---|
| Versión | V3 |
| Nº Serie (Serial Number) | Identificativo único del certificado |
| Algoritmo de Firma | Sha256WithRSAEncryption |
| Emisor (Issuer) | CN = ACA CA3<br>OI = VATES-Q2863006I<br>OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA<br>O = CONSEJO GENERAL DE LA ABOGACIA<br>C = ES |
| Valido desde (NotBefore) | (fecha de inicio de validez, tiempo UTC) |
| Valido hasta (NotAfter) (notAfter) | (fecha de fin de validez, tiempo UTC)<br>No superior a NotBefore + 825 días |
| Asunto (Subject) | Campos Obligatorios<br>CN < FQDN del servidor seguro><br>serialNumber = <CIF/NIF de la organización><br>O < Razón social de la organización que solicita el certificado><br>bussinesCategory(2.5.4.15)= Private Organization<br>jurisdictionOfIncorporationCountryName(1.3.6.1.4.1.311.60.2.1.3) = ES<br>L = <Localidad de la organización> - Opcional<br>ST = <Provincia de la organización> C = ES |
| Clave pública | RSA (2048 bits) |

#### 7.1.2.2 Extensiones

| **EXTENSIONES** | VALOR |
|---|---|
| Nombre alternativo del sujeto<br>(SubjectAlternativeName) | DNSName = <FQDN del servidor seguro><br>DNSName adicionales - Opcional |
| Restricciones básicas<br>(BasicConstraints) | Tipo de asunto= Entidad final<br>Restricción de longitud de ruta= Ninguno |

| | |
|---|---|
| Identificador de clave del titular<br>(SubjectKeyIdentifier) | 20 BYTE SHA-1 HASH (SUBJECTPUBLICKEY DEL CERTIFICADO) |
| Identificador de clave de entidad emisora<br>(AuthorityKeyIdentifier) | 3D D8 DD 01 BA C6 28 C5 4C B5 39 C2 F0 AD E6 D7 35 95 4F 2F |
| Uso mejorado de las claves<br>(ExtendedKeyUsage) | Autenticación del servidor (1.3.6.1.5.5.7.3.1)<br>Autenticación del cliente (1.3.6.1.5.5.7.3.2) -Opcional |
| Acceso a la Información de Autoridad<br>(Authority Information Access) | [1]Acceso a información de autoridad<br>Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)<br>Nombre alternativo:<br>Dirección URL=http://ocsp.redabogacia.org<br>[2]Acceso a información de autoridad<br>Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2)<br>Nombre alternativo:<br>Dirección URL=http://www.acabogacia.org/certificados/aca_ca3.crt |
| Directivas de certificado<br>(Certificate Policies) | Directiva de certificados:<br>Identificador de directiva= 1.3.6.1.4.1.16533.40.1.1<br>[1,1]Información de calificador de directiva:<br>Id. de calificador de directiva=CPS<br>Certificador:<br>http://www.acabogacia.org/doc<br>Identificador de directiva= 2.23.140.1.1 |
| Declaración de Certificados Calificados<br>qcStatements x.509v3 certificate extension from RFC 3039 | 1.- id-etsi-qcs-QcCompliance<br>2.- id-etsi-qcs-QcPDS<br>URL=http://www.acabogacia.org/doc/EN<br>Language = EN (ISO 639-1 language code)<br>3.- id-etsi-qct-web |
| Punto de distribución de la CRL<br>(CRLDistributionPoint) | http://www.acabogacia.org/crl/aca_ca3.crl<br>http://crl.acabogacia.org/crl/aca_ca3.crl |

| | |
|---|---|
| Uso de la Clave (KeyUsage) Campo crítico | Firma digital, 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.ç

### 7.2.2 CRL y extensiones

Los puntos de distribución son:

http://www.acabogacia.org/crl/aca_ca3.crl
http://crl.acabogacia.org/crl/aca_ca3.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 la Ley 59/2003 de Firma Electrónica y eIDAS, se informa a los suscriptores y usuarios de determinados aspectos en relación con dispositivos de creación y de verificación de firma electrónica que son compatibles con los datos de firma y con el certificado expedido, así como de mecanismos considerados seguros para la creación y verificación de firmas.

## *Dispositivos del suscriptor*

No aplica

## *Creación y verificación de firmas*

No aplica