Autoridad de Certificación de la Abogacía

Referencia: **CP7_ACA_004.0**
Fecha: **03/05/2017**
Estado del documento: **Publicado**

Consejo General de la Abogacía Española

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

CP7_ACA_004.0

CERTIFICADOS CUALIFICADOS DE ABOGADO EUROPEO

(VERSIÓN 004.0)

El presente documento no puede ser reproducido, distribuido, comunicado públicamente, archivado o introducido en un sistema de recuperación de información, o transmitido, en cualquier forma y por cualquier medio (electrónico, mecánico, fotográfico, grabación o cualquier otro), total o parcialmente, sin el previo consentimiento por escrito del Consejo General de la Abogacía Española.

Las solicitudes para la reproducción del documento o la obtención de copias del mismo deben dirigirse a:

Administración ACABOGACÍA
Consejo General de la Abogacía Española
Paseo de Recoletos, 13
28004 Madrid

Control del Cambios

Fecha	Versión	Cambios
01/10/2011	CP7_ACA_001.0	Versión inicial
13/03/2014	CP7_ACA_002.0	Se incluye una descripción de la Jerarquía PKI Se modifica el apartado de ámbito de aplicación y usos Se añade la posibilidad de renovación online Se elimina detalles del modelo de módulo Criptográfico Se indican los nuevos puntos de distribución de CRL Corrección de erratas
27/06/2016	CP7_ACA_003.0	Se incluye nueva Jerarquía PKI, información nuevos certificados CAs Se alinea con eIDAS Adaptación de servicios reconocidos a cualificados
03/05/2017	CP7_ACA_004.0	Se realiza la siguientemodificación del perfil del certificado: Se incluye el qctype Se modifica el KeyUsage para alinearlo con el ETSI EN 319 412 incluyendo no repudio, firma digital y cifrado de clave

Índice de Contenido

1. Introducción ____ *5*

1.1. Vista General ____ **5**

1.2. Identificación ____ **8**

1.3. Comunidad y Ámbito de Aplicación. ____ **8**

1.4. Datos de contacto ____ **12**

2. Cláusulas Generales ____ *13*

2.1. Obligaciones ____ **13**

2.2. Responsabilidad ____ **13**

2.3. Responsabilidad financiera ____ **14**

2.4. Interpretación y ejecución ____ **15**

2.5. Tarifas ____ **15**

2.6. Publicación y Registro de Certificados ____ **16**

2.7. Auditorias ____ **17**

2.8. Confidencialidad y Protección de Datos Personales ____ **17**

2.9. Derechos de propiedad intelectual ____ **18**

3. Identificación y Autenticación ____ *19*

3.1. Registro inicial ____ **19**

3.2. Renovación de certificados ____ **22**

3.3. Reemisión después de una revocación ____ **23**

3.4. Solicitud de revocación ____ **23**

4. Requerimientos Operacionales ____ *24*

4.1. Solicitud de certificados ____ **24**

4.2. Emisión de certificados ____ **24**

4.3. Aceptación de certificados ____ **25**

4.4. Suspensión y Revocación de certificados ____ **25**

4.5. Procedimientos de Control de Seguridad ____ **25**

5. Controles de Seguridad Física, Procedimental y de Personal ____ *26*

6. Controles de Seguridad Técnica ____ *27*

6.1. Generación e instalación del par de claves ____ **27**

6.2. Protección de la clave privada ____ **28**

6.3. Estándares para los módulos criptográficos ____ **29**

6.4. Ciclo de vida de los dispositivos criptográficos ____ **29**

6.5. Controles de seguridad ____ **29**

6.6. Controles de ingeniería de los módulos criptográficos ____ **30**

7. Perfiles de Certificado ____ *31*

7.1. Perfil de Certificado ____ **31**

7.2. Perfil de CRL ____ **37**

8. Especificación de la administración ____ *39*

8.1. Autoridad de las políticas ____ **39**

8.2. Procedimientos de especificación de cambios ____ **39**

8.3. Publicación y copia de la política ____ **39**

8.4. Procedimientos de aprobación de la Política ____ **39**

ANEXO 1: Información técnica ____ *40*

Dispositivos del suscriptor ____ **40**

Creación y verificación de firmas ____ **40**

Anexo 2: ACRONIMOS ____ *44*

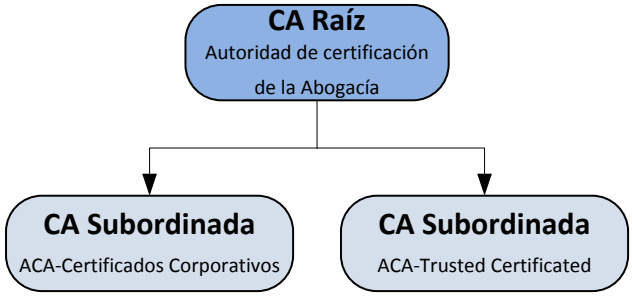
1. Introducción

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 Certificación mediante la creación de una jerarquía PKI propia. El Consejo General de la Abogacía Española se constituye en Prestador de servicios de Certificación mediante la creación de una jerarquía PKI propia. En este sentido, tal como establece la medida transitoria 3 del artículo 51 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 y por la que se deroga la Directiva 1999/93/CE, un prestador de servicios de certificación que emita certificados reconocidos conforme a la Directiva 1999/93/CE debe presentar un informe de evaluación de conformidad al organismo supervisor lo antes posible, pero no más tarde del 1 de julio de 2017. Hasta que el prestador de servicios de certificación presente dicho informe de evaluación de conformidad y el organismo supervisor ultime su análisis, el mencionado prestador de servicios de certificación será considerado como prestador cualificado de servicios de confianza.

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



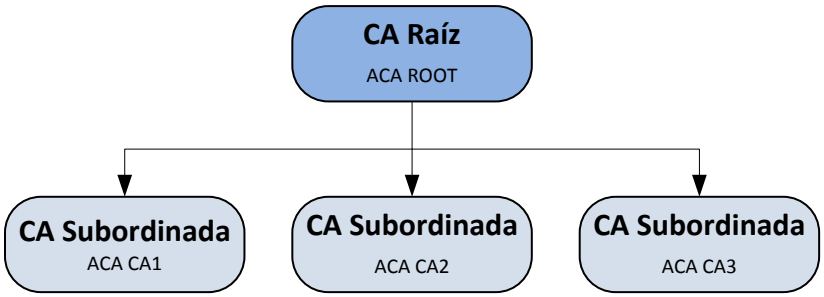
En el año 2014 se han generado nuevas CAs subordinadas con la misma denominación seguida del año de emisión: *ACA – Certificados Corporativos 2014 y ACA-Trusted Certificates 2014.*

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 Corporativo Cualificado de Abogado Europeo" 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 Cualificados y está basada en la especificación del estándar RCF 3647 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta estándares europeos, entre los que cabe destacar los siguientes:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- 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 (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
  (NOTA: Dicha Directiva será derogada cuando la gran mayoría del articulado de eIDAS sea aplicable, es decir, a partir del 1 de julio de 2016).
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015).
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal, como su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que en su Disposición final sexta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social, que en su disposición final cuarta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- 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.
- Real Decreto 951/2015, de 23 de octubre, de modificación del 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.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de Octubre de 2016).

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

Nombre:	CP7_ACA_004.0
O.I.D.	1.3.6.1.4.1.16533.10.9.1
Descripción:	Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: certificados cualificados de abogado europeo
Versión:	004.0
Fecha de Emisión:	03/05/2017
Localización:	www.acabogacia.org/doc

CPS relacionada	
O.I.D.	1.3.6.1.4.1.16533.10.1.1
Descripción:	Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Abogacía
Localización:	www.acabogacia.org/doc

1.3. Comunidad y Ámbito de Aplicación.

1.3.1 Autoridad de Certificación (AC)

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Usuario, en las relaciones electrónicas, vinculando una determinada clave pública con una persona (Suscriptor) relacionada a un Colegio Profesional concreto a través de la emisión de un Certificado.

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

1.3.2 Autoridad de Registro (AR)

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

A los efectos de la presente Política, las AR's son las siguientes entidades:

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

1.3.3 Prestador de servicios de certificación (PSC) / Prestador cualificado de Servicios de Confianza

Entendemos bajo la presente política a un PSC como aquella entidad que presta servicios concretos relativos al ciclo de vida de los certificados.

Las funciones de PSC pueden ser desempeñadas directamente por la AC o por una entidad delegada.

Por otro lado, tal como establece el apartado 3 de la medida transitoria del artículo 51 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 y por la que se deroga la Directiva 1999/93/CE, un prestador de servicios de certificación que emita certificados reconocidos conforme a la Directiva 1999/93/CE debe presentar un informe de evaluación de conformidad al organismo supervisor lo antes posible, pero no más tarde del 1 de julio de 2017. Hasta que el prestador de servicios de certificación presente dicho informe de evaluación de conformidad y el organismo supervisor ultime su análisis, el mencionado prestador de servicios de certificación será considerado como prestador cualificado de servicios de confianza.

Asimismo, los apartados 1 y 2 de la medida transitoria del artículo 51 del citado Reglamento establece que los dispositivos seguros de creación de firma cuya conformidad se haya determinado con arreglo a lo dispuesto en el artículo 3, apartado 4, de la Directiva 1999/93/CE se considerarán dispositivos cualificados de creación de firma electrónica con arreglo al presente Reglamento, y que los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/CE se considerarán certificados cualificados de firma electrónica con arreglo al presente Reglamento hasta que caduquen.

Por todo lo anterior, AC Abogacía, actúa como prestador cualificado de servicios de confianza, emitiendo certificados electrónicos cualificados de firma y proveyendo servicios de firma electrónica basados en certificados cualificados y creados mediante un dispositivo cualificado de creación de firma electrónica, conforme a lo establecido en el reglamento 910/2014 de la Unión Europea y en la Ley 59/2003 de Firma electrónica.

1.3.4 Suscriptor

Bajo esta Política el Suscriptor es una persona física, perteneciente a un Colegio de Abogados de España en calidad de colegiado ejerciente del mismo, poseedor de un "Certificado Corporativo cualificado de abogado europeo" alojado en un dispositivo cualificado de creación de firma electrónica. El suscriptor recibe también el nombre de "Firmante", según se define el art. 6 de la Ley 59/2003 y en el art. 3 de eIDAS.

1.3.5 Usuario

En esta Política se entiende por Usuario, tercera parte confiante, la persona que voluntariamente confía en el Certificado, en virtud de la confianza depositada en la AC, lo

utiliza como medio de acreditación de la autenticidad e integridad del documento firmado y en consecuencia se sujeta a lo dispuesto en esta Política, en la Declaración de Prácticas de Certificación (CPS) aplicable y la legislación vigente, por lo que no se requerirá acuerdo posterior alguno.

1.3.6 Solicitante

A los efectos de esta política el solicitante es la persona física que solicita el certificado cualificado de abogado europeo.

1.3.7 Ámbito de Aplicación y Usos

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

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

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

- Identificación del firmante y su condición de abogado: El Suscriptor del Certificado puede autenticar, frente a otra parte, su identidad y su condición de abogado, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado. El suscriptor podrá identificarse válidamente ante cualquier persona mediante la firma de un e-mail o cualquier otro fichero.
- Integridad del documento firmado: La utilización de este Certificado garantiza que el documento firmado es integro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Suscriptor. Se certifica que el mensaje recibido por el Usuario es el mismo que fue emitido por el Suscriptor
- No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Suscriptor que ha firmado no puede negar la autoría o la integridad del mismo.
- A pesar de ser posible su utilización para el cifrado de datos, no se recomienda la misma debido a que, no es posible la recuperación de los datos cifrados en caso de pérdida de la clave privada por parte del Suscriptor. El Suscriptor o el Usuario lo harán, en todo caso, bajo su propia responsabilidad.

Los certificados descritos en esta política son certificados cualificados, que además son conformes con lo establecido en el artículo 51 de eIDAS, que establece en el apartado segundo que, los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/CE se considerarán Certificados Cualificados de firma electrónica con arreglo al presente Reglamento hasta que caduquen. Estos certificados sirven de base para

la generación de firmas electrónicas cualificadas creadas mediante un dispositivo cualificado de creación de firmas electrónicas.
Por otro lado, son conformes con el art. 11 y 24 de la Ley 59/2003.

.

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

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

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

1.3.7.1 Límites y prohibiciones de uso de los certificados

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

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

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

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

El Suscriptor o el Usuario que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, la AC tenga responsabilidad alguna en el caso de cifrado de información usando las claves asociadas al certificado.

1.4. Datos de contacto

Organización responsable:
Autoridad de certificación de la Abogacía.
Consejo General de la Abogacía Española

Persona de contacto:
Administrador AC Abogacía
Departamento de Operaciones

E-mail:	info@acabogacia.org
Teléfono:	Tel. 902 41 11 41
Fax	915327836
Dirección:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

2. Cláusulas Generales

2.1. Obligaciones

2.1.1 AC

La AC se obliga según lo dispuesto en las Prácticas de Certificación así como lo dispuesto en la normativa sobre prestación de servicios de Certificación, la Ley 59/2003 y eIDAS, donde sean aplicables

2.1.2 AR

Las Autoridades de Registro son delegadas por la CA para realizar esta labor, por lo tanto la AR también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados.

2.1.3 Solicitante

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

2.1.4 Suscriptor

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

2.1.5 Usuario

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

2.1.6 Registro de Certificados

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

2.2. Responsabilidad

El Consejo General de la Abogacía Española, en su actividad de Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza responderá de acuerdo con el régimen de responsabilidad que establece la Ley 59/2003, de Firma Electrónica, eIDAS y el resto de la legislación aplicable.

En esta misma línea, la AC responderá según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

2.2.1 Exoneración de responsabilidad

La relación entre la AC y las AR se regirá por su especial relación contractual. La AC y las AR's se exonerarán de su responsabilidad en los términos establecidos en la Declaración de Prácticas de Certificación (CPS) y las políticas de certificación. En particular, la AC y las AR's no serán responsables en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

1. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la Declaración de Prácticas de Certificación (CPS), en particular por la utilización de un certificado suspendido o revocado, o por depositar la confianza en él sin verificar previamente el estado del mismo.

2. Por el uso indebido o fraudulento de los certificados o CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.

3. Por el uso indebido de la información contenida en el Certificado o en la CRL.

4. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Usuarios en la normativa vigente, la Declaración de Prácticas de Certificación (CPS) o en la Política de Certificación correspondiente.

5. Por el contenido de los mensajes o documentos firmados.

6. Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.

7. Fraude en la documentación presentada por el solicitante.

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

La AC limita su responsabilidad según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

2.3. Responsabilidad financiera

La AC, en su actividad como prestador cualificado de servicios de confianza mantiene recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad de Prestador tal como se establece la legislación aplicable.

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a 3.000.000 €.

2.4. Interpretación y ejecución

2.4.1 Legislación

La ejecución, interpretación, modificación o validez de la presente Política se regirá por lo dispuesto en la legislación española vigente.

2.4.2 Independencia

La invalidez de una de las cláusulas contenidas en esta Política no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

2.4.3 Notificación

Cualquier notificación referente a la presente Política se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

2.4.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

2.5. Tarifas

2.5.1 Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los usuarios en las diferentes Autoridades de Registro.

2.5.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos será gratuito, no obstante, la AC podrá imponer alguna tarifa para los casos de descarga masiva de certificados o cualquier otra circunstancia que a juicio de la AC deba ser gravada, en cuyo caso se publicarán dichas tarifas en la página web de la AC.

2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

La AC proveerá de un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito, por medio de la publicación de la CRL. No obstante, la AC podrá imponer alguna tarifa para otros medios de comprobación del estado de los

certificados o cualquier otra circunstancia que a juicio de la AC deba ser gravada, en cuyo caso se publicarán dichas tarifas en la página web de la AC.

2.5.4 Tarifas por otros servicios

Las tarifas aplicables a otros servicios se publicarán en la página web de la AC.

2.5.5 Política de reintegros

Sin estipulación.

2.6. Publicación y Registro de Certificados

2.6.1 Publicación de información de la AC

2.6.1.1 Políticas y Prácticas de Certificación

La presente Política de Certificación y sus distintas versiones estarán disponibles públicamente en el sitio de Internet http://www.acabogacia.org/doc

2.6.1.2 Términos y condiciones

AC Abogacía pondrá a disposición de los Suscriptores y Usuarios los términos y condiciones del servicio en el sitio de Internet http://www.acabogacia.org/doc

2.6.1.3 Difusión de los certificados

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

2.6.2 Frecuencia de publicación

AC Abogacía publicará de forma inmediata cualquier modificación en las políticas y 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.

2.6.3 Controles de acceso

AC Abogacía empleará diversos sistemas para la publicación y distribución de certificados y CRL's. Se necesitará tener unos datos de acceso para realizar consultas múltiples.

En la web de AC Abogacía existirán accesos al directorio para la consulta de CRL y Certificados bajo el control de una aplicación y protegiendo la descarga indiscriminada de información.

Las CRL's podrán descargarse de forma anónima mediante protocolo http.

2.7. Auditorias

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

2.8. Confidencialidad y Protección de Datos Personales

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

2.8.1 Tipo de información a mantener confidencial

La AC considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

2.8.2 Tipo de información considerada no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente Política y en las Prácticas de Certificación.
- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo de manera no exhaustiva:
    - Los certificados emitidos o en trámite de emisión.
    - La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza.
    - El nombre y los apellidos del suscriptor del certificado, en caso de certificados individuales, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.

- La dirección de correo electrónico del suscriptor del certificado, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de colectivo, o la dirección de correo electrónico asignada por el suscriptor, en caso de certificados para dispositivos.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.

- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.

2.8.3 Divulgación de información de revocación / suspensión de certificados

Se difundirá la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRLs. Los detalles del servicio se regirán por lo dispuesto en la Declaración de Prácticas de Certificación (CPS).

2.8.4 Envío a la Autoridad Competente

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

2.9. Derechos de propiedad intelectual

La propiedad intelectual de estas Políticas pertenece al CGAE. La AC será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita.

La AC concederá licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta política, y de acuerdo con el correspondiente instrumento vinculante entre el AC Abogacía y la parte que reproduzca y/o distribuya el certificado.

Las anteriores reglas figurarán en los instrumentos vinculantes entre la AC y los suscriptores y los terceros que confían en certificados.

3. Identificación y Autenticación

3.1. Registro inicial

3.1.1 Tipos de nombres

Todos los certificados requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.501.

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

- Un componente Nombre (Common Name) –CN
- Un componente E-mail –E
- Un componente Organización –O
- Un componente Unidad en la Organización –OU
- Un componente Título-T
- Un componente de ubicación geográfica -ST
- Un componente Estado (Country)-C
- Un componente Número de Serie –serialNumber
- Un componente Nombre de Pila (Given name)- G
- Un componente Apellido 1 “Surname” – SN
- Un componente Apellido 2 con OID 1.3.6.1.4.1.16533.30.1

Certificados de abogado europeo

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

- El valor autenticado del componente Organización –O contendrá el nombre del Colegio de Abogados al que pertenezca el suscriptor, y una referencia al código identificativo de la AR

- El valor autenticado del componente Unidad en la Organización –OU contendrá las siglas del Consejo General de la Abogacía y el número de colegiado del suscriptor

- El valor autenticado del componente Título-T contendrá el título del abogado según la denominación recogida en la Directiva 98/5/CE : Abogado/Advocat/Avogado/Abokatu

- El valor autenticado del componente de ubicación geográfica -ST contendrá el país donde se encuentra la AC. El contenido será "ES"

- El valor autenticado del componente Estado (Country)-C contendrá "ES"

- El valor autenticado del componente Número de Serie –serialNumber contendrá el NIF del suscriptor o identificador conforme ETSI EN 319 412-1.

- El valor autenticado del componente Nombre de Pila (Given name)- G contendrá el nombre de pila del Suscriptor

- El valor autenticado del componente Apellido 1 "Surname" –SN contendrá el primer apellido del Suscriptor

- El valor autenticado del componente con OID 1.3.6.1.4.1.16533.30.1 contendrá el segundo apellido del Suscriptor

3.1.2 Pseudónimos

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

3.1.3 Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.4 Unicidad de los nombres

Los nombres distinguidos de los certificados emitidos serán únicos para cada suscriptor. La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres de los certificados emitidos. El atributo del e-mail, el número de colegiado y/o el NIF se usarán para distinguir entre dos identidades cuando exista algún problema sobre duplicidad de nombres.

3.1.5 Procedimiento de resolución de disputas de nombres

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

La AC no tiene responsabilidad en el caso de resolución de disputas de nombres. El Prestador de Servicios de Certificación / 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 estipulado

3.1.7 Métodos de prueba de la posesión de la clave privada

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

La AR hace entrega (si no dispone de él) de un kit conteniendo el dispositivo cualificado de creación de firmas electrónicas. Si el dispositivo no ha sido previamente inicializado, el suscriptor inicializa en la propia AR y ante el operador el dispositivo cualificado de creación de firmas electrónicas. Durante este proceso se generan los datos de activación de del dispositivo, o si la inicialización se produce en una entidad externa, le serán entregados mediante un proceso que asegure la confidencialidad de los mismos ante terceros. La inicialización del dispositivo elimina totalmente cualquier información previa contenida en el mismo.

A continuación, el suscriptor genera el par de claves y un CSR en su dispositivo cualificado de creación de firmas electrónicas, enviando por un canal seguro la clave pública junto con los datos verificados a la AC en formato PKCS10 u otro equivalente. La generación del par de claves exigirá la introducción correcta de los datos de activación del dispositivo, y la introducción de un código de identificación del dispositivo que lo relaciona con el suscriptor autorizado a utilizarlo.
Por tanto el método de prueba de la posesión de la clave privada por el suscriptor será PKCS#10.

3.1.8 Autenticación de la identidad de un individuo

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

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

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

a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la AR en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en el párrafo primero y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b) Cuando para solicitar un certificado se utilice otro para cuya expedición se hubiera identificado al firmante en la forma prescrita en el párrafo primero y le conste a la AR que el período de tiempo transcurrido desde la identificación es menor de cinco años.

3.1.9 Requerimientos aplicables a las AR's externas

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

- Que existe un contrato en vigor entre la AC y la AR, concretando los aspectos concretos de la delegación y las responsabilidades de cada agente.
- Que la identidad de la AR y de los operadores de la AR ha sido correctamente comprobada y validada.
- Que los operadores de la AR han recibido formación suficiente para el desempeño de sus funciones.
- Que la AR asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones.
- Que la comunicación entre la AR y la AC, se realiza de forma segura mediante el uso de certificados digitales.
- Que las ARs se comprometen a cumplir con los requerimientos generales de seguridad indicados por la AC.

3.2. Renovación de certificados

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

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

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

3.3. Reemisión después de una revocación

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

3.4. Solicitud de revocación

Pueden solicitar la suspensión o revocación de un certificado:

- El propio suscriptor, en cuyo caso deberá facilitar la clave de revocación que se le entregó junto con el certificado, o deberá identificarse ante la AR según lo establecido en el apartado correspondiente.

- Los operadores autorizados de la AR del suscriptor.

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

En cualquiera de los dos últimos casos deberán concurrir las circunstancias que se establecen en el apartado establecido por la 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

4.1. Solicitud de certificados

Las AR's gestionan las solicitudes de certificados digitales.

La solicitud de un certificado digital podrá realizarse personándose el suscriptor en su Colegio de Abogados o en el Consejo General de la Abogacía ante un operador debidamente autorizado.

Antes de iniciar el proceso de emisión, la AR informa al solicitante del proceso de emisión, las responsabilidades y las condiciones de uso del certificado y del dispositivo, así como verifica la identidad del solicitante, y los datos a incluir en el certificado.

Si la verificación es correcta se procede a la firma del instrumento jurídico vinculante entre el solicitante y la AC – AR, convirtiéndose el solicitante en suscriptor.

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

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

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

4.2. Emisión de certificados

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

- La AR recibe la petición de emisión del certificado.

- El operador de la AR verifica nuevamente el contenido del mismo y si la verificación es correcta lo valida y tramita la aprobación de la emisión para la AC, mediante la firma digital de la petición con su certificado de operador. Si la petición no es correcta, el operador deniega la petición.
- La AR envía por un canal seguro la petición a la AC para la emisión del correspondiente certificado.
- La AC emite el certificado, si la petición recibida no contiene errores técnicos, en el formato o contenido de la misma, vinculando de forma segura el certificado con la información de registro, incluyendo la clave pública certificada, en un sistema que utiliza protección contra falsificación y mantiene la confidencialidad de los datos intercambiados.
- El certificado generado es enviado de forma segura a la AR, para proceder a su descarga en el Dispositivo cualificado de creación de firmas electrónicasen presencia del Suscriptor.
- La AC notifica al suscriptor la emisión del mismo.
- El certificado generado es enviado de forma segura al Registro de Certificados, que lo pone a disposición de los usuarios. Aceptación de certificados

Con la entrega de la tarjeta con el certificado, el suscriptor acepta su certificado en el dispositivo cualificado de creación de firmas electrónicasque custodia la clave privada.

4.3. Aceptación de certificados

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

4.4. Suspensión y Revocación de certificados

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

4.5. Procedimientos de Control de Seguridad

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

5. Controles de Seguridad Física, Procedimental y de Personal

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

6. Controles de Seguridad Técnica

6.1. Generación e instalación del par de claves

6.1.1 Generación del par de claves del suscriptor

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

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

El dispositivo cualificado de creación de firmas electrónicas utiliza una clave de activación para el acceso a las claves privadas. En caso de que la entrega del dispositivo no se realice de manera presencial en la AR, los datos de activación se entregarán mediante un proceso que asegure la confidencialidad de los mismos ante terceros. En ningún caso, las ARs custodiaran los datos de activación del dispositivo cualificado de creación de firmas electrónicas.

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

6.1.2 Entrega de la clave pública al emisor del certificado

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

6.1.3 Entrega de la clave pública de la CA a los Usuarios

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

6.1.4 Tamaño y periodo de validez de las claves

6.1.4.1 Tamaño y periodo de validez de las claves del emisor

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

6.1.4.2 Tamaño y periodo de validez de las claves del suscriptor

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

El periodo de uso de la clave pública y privada del suscriptor puede corresponder con la validez temporal de los certificados, no pudiendo ser en ningún caso superior a 3 años.

6.1.5 Parámetros de generación de la clave pública

No estipulado.

6.1.6 Comprobación de la calidad de los parámetros

No estipulado.

6.1.7 Hardware/software de generación de claves

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

Las claves de los suscriptores son generadas mediante dispositivos cualificados de creación de firmas electrónicas. El dispositivo SSCD ha sido evaluado según el Perfil de Protección - Secure Signature Creation Device Type 3, versión 1.05, de acuerdo con CC, version 3.1 révision 3, hasta un Nivel de Garantía de Evaluación EAL 4 aumentado con AVA_VAN.5. En conformidad con el apartado 1 de la medida transitoria del artículo 51 del Reglamento 910/2014 (eIDAs), los dispositivos seguros de creación de firma cuya conformidad se haya determinado con arreglo a lo dispuesto en el artículo 3, apartado 4, de la Directiva 1999/93/CE se considerarán dispositivos cualificados de creación de firma electrónica con arreglo al presente Reglamento.
Las claves de las CA vinculadas son generadas en un módulo criptográfico validado FIPS 140-2 nivel 3.

6.1.8 Fines del uso de la clave

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

6.2. Protección de la clave privada

Clave privada de la AC

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

Clave privada del suscriptor

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

6.3. Estándares para los módulos criptográficos

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

6.4. Ciclo de vida de los dispositivos criptográficos

6.4.1 Ciclo de vida de los dispositivos cualificados de creación de firma electrónica (DCCFE)

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

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

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

6.5. Controles de seguridad

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

6.6. Controles de ingeniería de los módulos criptográficos

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

7. Perfiles de Certificado

7.1. Perfil de Certificado

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

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

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica;
b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y
— para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
— para personas físicas, el nombre de la persona;
c) al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;
d) datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;
e) los datos relativos al inicio y final del período de validez del certificado;
f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;
g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);
i) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;
j) cuando los datos de creación de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

7.1.1 Descripción del perfil

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

Certificados emitidos por ACA - Certificados Corporativos

CAMPOS	
Versión	V3
Nº Serie (Serial)	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)
Algoritmo de Firma	Sha1WithRSAEncryption
Emisor (issuer)	CN = ACA - Certificados Corporativos OU = Autoridad de 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 (2048 bits)

Certificados emitidos por ACA - Certificados Corporativos 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 - Certificados Corporativos - 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 CA1

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 CA1 OI = VATES-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)

7.1.2 Extensiones del certificado

Se incluirán las siguientes extensiones:

Certificados emitidos por ACA - Certificados Corporativos

EXTENSIONES	
Nombre alternativo del emisor (IssuerAlternativeName)	Nombre RFC822=ac@acabogacia.org Dirección URL=http://www.acabogacia.org
Nombre alternativo del sujeto (SubjectAlternativeName)	Nombre RFC822=xxxx.xxxxx@cgae.es
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos, Contrato de claves
Uso mejorado de las claves (ExtendedKeyUsage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Tipo de certificado Netscape (NetscapeCertType)	Autenticación del cliente SSL, SMIME (a0
URL de directiva de entidad emisora de certificados de Netscape (netscape-ca-policy-url)	http://www.acabogacia.org/doc
Comentario de Netscape	Este es un certificado personal reconocido. Consulte

(NetscapeComment)	http://www.acabogacia.org/doc
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	5a794ca10cfc08162cc285454f 32abe72b45c011
Identificador de clave de asunto (SubjectKeyIdentifier)	
Bases de certificado (SubjectStatement)	Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.10.9.1 [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 Calificador: Texto de aviso=Este es un certificado personal reconocido. Consulte http://www.acabogacia.org/doc
Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/acacorporativos.crl http://crl.acabogacia.org/crl/acacorporativos.crl
Restricciones básicas (BasicConstraints)	Tipo de asunto= Entidad final Restricción de longitud de ruta= Ninguno
Acceso a la Información de Autoridad (Authority Information Access)	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.acabogacia.org/certificados/ACAcorporativos.crt
1.3.6.1.5.5.7.1.3 qcStatements x.509v3 certificate extension from RFC 3039	0 Euros

Certificados emitidos por ACA - Certificados Corporativos 2014

EXTENSION	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)	33 6D D0 E9 CD 18 D7 B4 EB 4E FC F3 E3 CD FB 3D 5B C0 A3 9E
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	[1]Acceso a información de autoridad

(Authority Information Access)	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/ACAcorporativosv2.crt
Directivas de certificado (Certificate Policies)	Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.10.9.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc
Declaración de Certificados Calificados qcStatements x.509v3 certificate extension from RFC 3039	1.- id-etsi-qcs-QcCompliance 2.- id-etsi-qcs-QcSSCD
Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/acacorporativosv2.crl http://crl.acabogacia.org/crl/acacorporativosv2.crl
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos, Contrato de claves

Certificados emitidos por ACA CA1

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)	72 A9 E7 D6 8E 02 67 A0 4A 4C 1A 67 31 BC B7 FE CB 84 B4 9B

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_ca1.crt
Directivas de certificado (Certificate Policies)	Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.10.9.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc
Declaración de Certificados Calificados qcStatements x.509v3 certificate extension from RFC 3039	1.- id-etsi-qcs-QcCompliance 2.- id-etsi-qcs-QcSSCD 3.- id-etsi-qcs-QcPDS URL=http://www.acabogacia.org/doc/EN
Punto de distribución de la CRL (CRLDistributionPoint)	http://www.acabogacia.org/crl/aca_ca1.crl http://crl.acabogacia.org/crl/aca_ca1.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 Restricciones de los nombres

No estipulado.

7.2. Perfil de CRL

7.2.1 Número de versión

Las CRL emitidas por la AC son de la versión 2.

7.2.2 Periodo de Emisión y validez

Se emiten de oficio diariamente y cuando sufra un cambio de estado. La validez es semanal.

7.2.3 Publicación.

La publicación es inmediata a su emisión.

Los puntos de distribución son:

Para certificados emitidos con la CA ACA- Corporativos

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

Para certificados emitidos con la CA ACA- Corporativos 2014

http://www.acabogacia.org/crl/ACAcorporativosV2.crl
http://crl.acabogacia.org/crl/ACAcorporativosV2.crl

Para certificados emitidos con la ACA CA1

http://www.acabogacia.org/crl/aca_ca1.crl
http://crl.acabogacia.org/crl/aca_ca1.crl

7.2.4 CRL y extensiones

Se incluirán las siguientes extensiones

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

8. Especificación de la administración

8.1. Autoridad de las políticas

El CGAE es el responsable del mantenimiento de las políticas de certificación, y puede ser contactado en la dirección especificada en el apartado 1.

8.2. Procedimientos de especificación de cambios

Todos los cambios propuestos que puedan afectar sustancialmente a los usuarios de esta política serán notificados inmediatamente a los suscriptores mediante la publicación en la web de AC Abogacía, haciendo referencia expresa en la "página principal" de la misma a la existencia del cambio.

Los usuarios afectados podrán presentar sus comentarios a la organización de la administración de las políticas dentro de los 45 días siguientes a la recepción de la notificación.

8.3. Publicación y copia de la política

Una copia de esta Política estará disponible en formato electrónico en la dirección de Internet: http://www.acabogacia.org/doc. Las versiones anteriores serán retiradas de su consulta on-line, pero pueden ser solicitadas por los interesados en la AC Abogacía.

8.4. Procedimientos de aprobación de la Política

La publicación de las revisiones de esta política deberá ser aprobada por el CGAE.

ANEXO 1: Información técnica

En cumplimiento de lo establecido en la Ley 59/2003 de Firma Electrónica 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

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

A. Dispositivos Cualificados de Creación de Firma Electrónica:

Los Certificados cualificados identificados por el OID de Política 1.3.6.1.4.1.16533.10.9.1 requieren, para su emisión que los datos de creación de firma hayan sido generados por el suscriptor y se custodien en un dispositivo que cumple lo establecido en el Anexo II de eIDAS, y que se denominan "Dispositivos cualificados de Creación de Firmas Electrónicas (DCCFE)".

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

La AC considera adecuados los dispositivos que cumplan lo siguiente:

- Que dispongan de la correspondiente certificación de dispositivo según lo establecido en el artículo 51 de eIDAS, en cuyo caso se admitirá sin más.

B. Otros Dispositivos de Creación de Firma:

No estipulado

En ambos casos (A) y (B), la AC sólo emitirán certificados respondiendo a las solicitudes que cumplan con lo establecido en el apartado siguiente para los algoritmos de generación de clave y parámetros del algoritmo de firma considerados adecuados (Claves RSA de 2048 bits) aunque el dispositivo disponga de la capacidad técnica para generar otro tipo de conjunto de parámetros de firma.

Creación y verificación de firmas

Estándares y parámetros admitidos

El uso correcto de los dispositivos para la creación de Firmas Electrónicas consideradas seguras, queda asociado a la utilización de un subconjunto de estándares y parámetros de entre los aprobados por la ETSI en el documento "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"" ETSI TS 119 312 y "Electronic Signatures and Infrastructures (ESI);
Guidance on the use of standards for cryptographic suites" ETSI TR 119 300 (www.etsi.org)

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

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

Métodos de verificación de firmas

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

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

- Es necesario utilizar un dispositivo apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizadas en el certificado y/o ejecutar cualquier otra operación criptográfica. 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 ETSI EN 319 122-2 "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures" del European Telecommunications Standards Institute (www.etsi.org), que AC Abogacía recomienda.
- Utilización por el firmante y el verificador de servicios de mediación de terceras partes, en los que ambos depositen su confianza, como:
    - Servicios de validación de certificados
    - Servicios de sellado de tiempo
    - Servicios de notarización de transacciones
    - Etc
- Conservación, de manera segura e íntegra, junto con la firma de todos los datos necesarios para su verificación:
    - Todos los certificados de la cadena de certificación.
    - Todas las CRL vigentes inmediatamente antes y después del momento de la firma.
    - Las políticas y prácticas en vigor en el momento de la firma.

Anexo 2: ACRONIMOS

AC	Autoridad de Certificación, también puede encontrarse identificada por el acrónico CA (*Certification Authority*)
ACA	Autoridad de Certificación de la Abogacía
AR	Autoridad de Registro también puede encontrarse identificada por el acrónico RA (*Registration Authority*)
ARL	*Authority Revocation List*, lista de certificados revocados de la Autoridad de Certificación Raíz
CGAE	Consejo General de la Abogacía Española
CPS	*Certification Practice Statement*, Declaración de Practicas de Certificación. también puede encontrarse identificada por el acrónico DPC
CRL	*Certificate revocation list*, Lista de certificados revocados
CSR	*Certificate Signing request*, petición de firma de certificado
DES	*Data Encryption Estándar*. Estándar de cifrado de datos
DN	*Distinguished Name*, nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm*. Estándar de algoritmo de firma
DSCF/	Dispositivo Seguro de Creación de Firma
DCCFE	Dispositivo Cualificado de Creación de Firmas Electrónicas
eIDAS	Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
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-256	*Secure Hash Algorithm*. Algoritmo seguro de Hash
TLS	*Transport Layer Security. Su antecesor es SSL (Secure Socket Layer, es un* protocolo diseñado por Netscape y convertido en estándar en la Red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor).
TCP/IP	*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.