

# **POLÍTICA DE CERTIFICADOS DE LA AUTORIDAD CERTIFICADORA RAÍZ DE LA SECRETARÍA DE ECONOMÍA**

Noviembre 2005

## **1. INTRODUCCIÓN**

La Política de Certificados, es un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad y clase de aplicaciones con requerimientos comunes de seguridad.

En este documento se describe la Política de Certificados para la Autoridad Certificadora Raíz de la Secretaría de Economía (ACR-SE). La Política de Certificados se aplica a la solicitud, validación, aceptación, emisión o revocación de los certificados digitales dentro de una Infraestructura de Clave Pública (PKI por sus siglas en inglés).

La ACR-SE, a través de la Dirección General de Normatividad Mercantil (DGNM), certificará las claves públicas de las Autoridades Certificadoras que hallan sido acreditados por la DGNM.

## **2. ALCANCE**

De acuerdo a la estructura jerárquica de certificación descrita en el apartado COMUNIDAD Y APLICABILIDAD DE LA ACR-SE, la ACR-SE podrá certificar la clave pública de autoridad certificador a:

- a) La Dirección General de Normatividad Mercantil (CD-ACDGNM). Ésta a su vez podrá certificar las clave públicas de autoridades certificadoras para Instituciones Públicas Gubernamentales; para entidades de la SE; de identidad personal (CD-IP) para funcionarios públicos de la SE y para los particulares que realicen trámites ante esta Secretaría.
- b) SIGER (CD-ACSIGER). Ésta a su vez podrá certificar las clave públicas de los RPC y fedatarios públicos.
- c) Prestadores de Servicios de Certificación (CD-ACPSC), que hayan sido acreditadas por la DGNM y cuya Política de Certificados sea tan restrictiva como lo descrito en este documento. Éstos podrán certificar las claves públicas de personas físicas o morales para efectos comerciales, entre otros.

La Autoridad Certificadora Raíz de la SE, se establece para crear y desarrollar una PKI a nivel nacional para el desarrollo del comercio electrónico.

## **3. REFERENCIAS**

- RFC 3647 -Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, noviembre 2003. <http://www.fqs.org/rfcs/rfc3647.html>
- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile abril 2002, <http://www.fqs.org/rfcs/rfc3280.html>.
- ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection

--The Directory: Public-key and attribute certificate frameworks.

- Código de Comercio, publicado el 29 de agosto de 2003, en el Diario Oficial de la Federación.
- REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación, Publicado el 19 de julio de 2004 en el Diario Oficial de la Federación
- REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación. Publicadas el 10 de agosto de 2004, en el Diario Oficial de la Federación.

#### 4. DEFINICIONES

**Certificado:** Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

**Comunidad:** Estará integrada por los Prestadores de Servicios de Certificación, acreditados por la DGNM, Instituciones Públicas Gubernamentales y áreas que integran la Secretaría de Economía.

**Emisor:** Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

**Firma Electrónica:** Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

**Firma Electrónica Avanzada o Fiable:** Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97, del CoCo. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

**Prestador de Servicios de Certificación:** La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

**Secretaría:** Se entenderá la Secretaría de Economía.

**Titular del Certificado:** Se entenderá a la persona a cuyo favor fue expedido el certificado.

#### 5. ABREVIACIONES:

**ACR-SE** Autoridad Certificadora Raíz de la Secretaría de Economía.

**CoCo** Código de Comercio.

**RGPSC** Reglas Generales de Prestadores de Servicios de Certificación.

**CD-IPAC** Certificados Digitales de Identidad Personal para sus Agentes Certificadores de la Secretaría de Economía.

**CD-IP** Certificados Digitales de Identidad Personal.

**CD-ACPSC** Certificados Digitales de Autoridad Certificadora de Prestadores de Servicios de Certificación.

**CD-ACSIGER** Certificado Digitales de Autoridad Certificadora de Sistema Integral de Gestión Registral.

**CD-ACDGNM** Certificado Digitales de Autoridad Certificadora de la Dirección General de Normatividad Mercantil.

**CD-ACIPG** Certificados Digitales de Autoridad Certificadora de Instituciones Publicas Gubernamentales.

**DGNM** Dirección General de Normatividad Mercantil.

**RPSC** Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

**LCR** Lista de Certificados Revocados.

**OCSP** Protocolo de Estatus de Certificados en Línea (por sus siglas en inglés).

**CLAVES** Clave Pública y Clave Privada.

**RA-SE** Autoridad Registradora de la Secretaría de Economía

**PSC** Prestadores de Servicios de Certificación

**URL** "Uniform Resource Locator", Localizador uniforme de recurso

## **6. IDENTIDAD DE LA ACR-SE**

Distinguished Name (DN): C=MX, O=Secretaría de Economía, OU=Dirección General de Normatividad Mercantil, CN=ACR-SE/

Ubicación: Insurgentes Sur #1940, 1er. Piso, Del. Álvaro Obregón  
C.P. 01030, México, D.F.

Correo electrónico de la ACR-SE: [acrse@economia.gob.mx](mailto:acrse@economia.gob.mx)  
Teléfono (+52) (55) 52.29.61.00 ext. 33533

Fax : 52.29.91.00 ext. 33599

Información sobre la Infraestructura de Clave Pública de la ACR-SE:  
<http://ac.economia.gob.mx.gob.mx>

## 7. COMUNIDAD Y APLICABILIDAD DE LA ACR-SE

La comunidad y aplicabilidad de la ACR-SE están determinadas en esta Política de Certificados. La ACR-SE emitirá certificados de identidad personal (CD-IPAC) para sus agentes certificadores; certificados digitales de autoridad certificadora (CD-ACPSC) a las autoridades certificadoras de las personas físicas y morales de carácter privado o público que hayan sido acreditados como Prestadores de Servicios de Certificación por la DGNM; a la Autoridad Certificadora (CD-ACSIGER) a del SIGER para el ámbito del Registro Público de Comercio y a las autoridades certificadoras de las áreas que integran a la Secretaría de Economía.

Solo emitirá otro tipo de certificado digital, en caso de ser necesario para la operación de alguna necesidad de la Secretaría de Economía. Éste deberá ser autorizado por el Comité de Seguridad de la DGNM.

### 7.1. ESTRUCTURA JERÁRQUICA

La estructura jerárquica de certificación se compone de los siguientes elementos:

1. **Autoridad Certificadora Raíz de la Secretaría de Economía**.- Ofrece servicios de certificación de clave pública de las autoridades certificadoras subordinadas a la ACR-SE de la SE. La SE es una institución pública gubernamental establecida para el desarrollo del ámbito comercial, tanto en el Registro Público de Comercio como para el comercio electrónico, entre otros.
2. **Autoridades Certificadoras Subordinadas** de la **ACR-SE** de la Secretaría de Economía.- Serán las personas físicas o morales acreditadas como PSC, instituciones públicas gubernamentales, direcciones generales de la SE, de acuerdo al CoCo, RPSC, RGPSC y a esta Política de Certificados.
3. **Agentes Certificadores** de la Autoridad Certificadora Raíz de la Secretaría de Economía.- Serán los encargados de emitir los certificados digitales, a las entidades subordinadas de la ACR-SE.
4. **Autoridad Registradora** de la Autoridad Certificadora Raíz de la
5. Secretaría de Economía.- Será la encargada de la autenticación de documentos e identificación de los solicitantes y titulares del certificado digital de la autoridad certificadora y de completar el procedimiento definido

para la emisión de los certificados Anexo I.

## **8. PRIVACIDAD Y SEGURIDAD**

### **8.1. REQUERIMIENTOS DE SEGURIDAD PARA LA ACR-SE Y SUS CLAVES.**

- La ACR-SE operará en un servidor de misión crítica redundante desconectado de la red, el intercambio de información con sus entidades subordinadas será mediante dispositivos de almacenamiento removible, únicamente para efectos de certificación de las mismas.
- El intercambio de información entre el servidor WEB de la ACR-SE con los Autoridades Certificadoras Subordinadas, será en los términos establecidos en las reglas de la 5 a la 5.3 de las RGPSC.
- La clave privada de la ACR-SE estará en todo momento cifrada, en un dispositivo de alta seguridad que cumpla con la norma FIPS 140-2 nivel 3.
- Tanto el *hardware* como el *software* que opera la ACR-SE se mantendrá en todo momento físicamente seguro.
- El par de claves RSA de la ACR-SE tendrá una longitud de 2048 bits.
- Se establecerá un procedimiento periódico de respaldo de los servidores que opere la ACR-SE. Las copias se guardarán en un lugar seguro, protegido de accesos no autorizados.
- Si la clave privada de la ACR-SE estuviera comprometida, se procedería a la revocación de la misma y del certificado de la ACR-SE, así como todos los certificados emitidos por ella, no importando la fecha de emisión. A partir de ese momento, deberán revocarse todos los certificados emitidos por las Autoridades Certificadoras Subordinadas ala ACR-SE y no deberán emitir certificados válidos hasta que no se restaure la identidad de la ACR-SE y se vuelvan a generar certificados respectivos a las Autoridades Certificadoras Subordinadas.

### **8.2. REQUERIMIENTOS DE SEGURIDAD IMPUESTOS A LAS AUTORIDADES CERTIFICADORAS SUBORDINADAS Y SUS CLAVES.**

- Las Autoridades Certificadoras operarán en un servidor de misión crítica redundante.
- Éste servidor podrá estar conectado a la red, en tal caso, el intercambio de información se hará entre el servidor y sus usuarios por lo menos vía SSL o la tecnología que ofrezca mayor seguridad, asimismo, deberá deshabilitar todos los servicios de red que no se requieran para el buen funcionamiento del servicio, manteniendo
- seguros y monitoreados aquellos que sean necesarios.
- La clave privada de la Autoridad Certificadora estará cifrada en un dispositivo que cumpla con el estándar FIPS 140 nivel 3.
- Tanto el *hardware* como el *software* del servidor de misión crítica que opera la Autoridad Certificadora se mantendrá en todo momento físicamente seguro.
- El par de claves RSA de una Autoridad Certificadora tendrá como mínimo una longitud de 2048 bits.
- El par de claves RSA de los certificados emitidos por las Autoridades Certificadora Subordinadas tendrá como mínimo una longitud de 1024 bits.

## **9. LA AUTORIDAD CERTIFICADORA ACR-SE:**

La ACR-SE es la instancia de la Secretaría de Economía, encargada de certificar la clave pública de las Autoridades Certificadoras Subordinadas, de acuerdo al Código de Comercio, Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y sus Reglas Generales. Así como de emitir o revocar los certificados de las autoridades referidas como se menciona en el apartado "ALCANCE", para más información consultar:

<http://ac.economia.gob.mx>.

<http://www.economia.gob.mx>.

## **10. POLITICA DE CERTIFICACIÓN**

### **10.1.POLÍTICA DE SEGURIDAD**

El objetivo de la ACR-SE será únicamente la emisión y revocación de certificados citados en el apartado "ALCANCE" y Certificados Digitales de Servidores, Certificados Digitales de Autoridad Certificadora de Estampas de Tiempo.

Se emitirán CD-IPAC para sus Agentes Certificadores.

Se emitirán CD-ACPSC para aquellos PSC que hayan sido acreditados por la DGNM, en términos del CoCo, RPSC y RGPSC, y que hayan presentado su solicitud de certificado. Se emitirán también CD-ACSIGER, CD-ACDGNM y CD-ACIPG para las Autoridades correspondientes.

La revocación de cualquier certificado se realizará de acuerdo a lo establecido en el apartado "REVOCAIONES".

Las Autoridades Certificadoras subordinadas de la ACR-SE, emitirán Certificados Digitales de Identidad Personal, Certificados Digitales de Servidores, Certificados Digitales de Autoridad Certificadora de Estampas de Tiempo, y Certificados Digitales para Agentes Certificadores dentro de la misma Autoridad Certificadora Subordinada.

Sólo se emitirán Certificados Digitales de Servidores a para los equipos que pertenezcan a las ACR-SE.

### **10.2.PERÍODO DE VALIDEZ DE LOS CERTIFICADOS DIGITALES**

El período de validez del Certificado Digital de la ACR-SE no será menor a 10 años a partir de su fecha de emisión.

El período de validez de los Certificados Digitales de Autoridad Certificadora subordinada no será menor de 10 años a partir de su fecha de emisión, igualmente para los certificados de servidor.

Cuando se haya superado cuatro quintos del tiempo de vida de la ACRSE, se generará un nuevo certificado digital y en su caso una nueva identidad. A partir de ese momento, las nuevas inscripciones se harán firmando certificados con esa nueva identidad. De este modo las Autoridades Certificadoras Subordinadas dispondrán de una quinta parte del tiempo para solicitar nuevos certificados a la nueva identidad.

### **10.3.CONVENCIONES DE NOMBRES**

Cada Autoridad Certificadora deberá asegurar que su DN (*Distinguished Names*) sea único, en función de que será el DN que tendrán los certificados que emita.

El *CountryName* deberá ser "mx".

Cada Autoridad Certificadora Subordinada, tiene que establecer mecanismos que aseguren la unicidad de los DN (*Distinguished Names*) de los certificados digitales que emita.

C= <CountryName>

O= <OrganizationName>

CN= <CommonName>

## **11. DISPOSICIÓN DE CERTIFICADOS**

Cada Autoridad Certificadora debe mantener un repositorio o base de datos con los certificados que emita, de manera que estén disponibles al público a través de un servicio de distribución de certificados.

Así mismo, la ACR-SE mantendrá constancia, en las páginas Web habilitadas para tal fin, de los certificados emitidos o revocados por ésta.

## **12. LISTA DE CERTIFICADOS REVOCADOS (LCR)**

Las LCRs (Listas de Certificados Revocados) deben ser firmadas por lo menos con la periodicidad establecida en la regla 2.4.8.1.5 de las RGPSC, por las Autoridades Certificadoras Subordinadas a ésta. Las Autoridades Certificadoras subordinadas serán responsables de indicar en los certificados que emita, la dirección en Internet (URL siglas en inglés) de su página en donde se localizará la Lista de Certificados Revocados y el Protocolo de Estatus de Certificados en Línea (OCSPs), para que de esta manera sea fácilmente accesible por los usuarios.

Toda Autoridad Certificadora se comprometerá a mantener actualizada la LCR y la OCSP, incluyendo todos los certificados revocados desde la última actualización.

## **13. OBLIGACIONES**

### **13.1.OBLIGACIONES DE LA DGNM COMO GESTOR DE LA ACR-SE:**

- Ofrecer y mantener la infraestructura necesaria para el establecimiento de una estructura jerárquica de certificación de Autoridades Certificadoras, según la Política de Certificados descrita en este documento.
- Implementar y mantener los requerimientos de seguridad impuestos a las claves de la ACR-SE, según lo descrito en este documento en el apartado "PRIVACIDAD Y SEGURIDAD".
- Aprobar o denegar las solicitudes de de acreditación así como de certificados y, en el primer caso, emitir los certificados de acuerdo con lo establecido en el apartado "POLÍTICA DE SEGURIDAD" de este documento.
- Poner copias de sus propios certificados y de cualquier información de

revocación a disposición de quien desee verificar una firma electrónica avanzada con referencia a dichos certificados. Para ello, se publicará y se mantendrá actualizada dicha información en las páginas Web destinadas a la infraestructura de certificación (Ver apartado "IDENTIDAD DE LA ACR-SE")

- Revocar los certificados según el procedimiento establecido en el apartado "REVOCAIONES" de este documento.
- Mantener actualizada la LCR, incluyendo todos los certificados revocados desde la última actualización.
- Proteger los datos de carácter personal que sean suministrados por los solicitantes a acreditación de PSC, de acuerdo con la Ley de Transparencia y de Acceso a la Información Pública Gubernamental.
- Comunicar inmediatamente, a los profesionales informáticos y responsables directos de las Autoridades Certificadoras, el compromiso, pérdida, divulgación, modificación, uso no autorizado de la clave privada de la ACR-SE, con el fin de restaurar la jerarquía lo antes posible según lo establecido en el apartado "PRIVACIDAD Y SEGURIDAD" de este documento.

### **13.2.OBLIGACIONES DE LA RA-SE DE LA ACR-SE**

La Autoridad Registradora de la ACR-SE:

- Llevará a cabo cada uno de los pasos descritos en el procedimiento de emisión de certificados digitales por parte de la ACR-SE para las Autoridades Certificadoras, según lo descrito en el **anexo I** de este documento.
- Llevará a término la identificación y autenticación para la revocación de certificados, de acuerdo con los procedimientos de validación establecidos en el apartado "REVOCAIONES" de este documento.
- Protegerá los datos personales de los solicitantes de certificados digitales, que no podrán ser cedidos a terceros bajo ningún concepto de acuerdo a la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental.

### **13.3.OBLIGACIONES DE LAS AUTORIDADES CERTIFICADORAS SUBORDINADAS.**

- Toda Autoridad Certificadora y sus correspondientes Autoridades Registradoras deben conocer la Política de Certificados de la ACR-SE, comprometiéndose a seguir las siguientes normas:
- Una Autoridad Certificadora en ningún caso emitirá certificados con una duración superior a la vigencia del vínculo administrativo existente entre el solicitante y la misma Autoridad Certificadora.
- Toda Autoridad Certificadora se compromete y obliga a enviar una copia a la ACR-SE, de los certificados emitidos de acuerdo a lo establecido en la regla 5 de las RGPSC, asimismo copia de su última LCR firmada.
- Toda Autoridad Certificadora se compromete y obliga a proteger sus claves secretas utilizadas en la emisión de certificados con el nivel de seguridad que se especifica en este documento en el apartado "REQUERIMIENTOS DE SEGURIDAD IMPUESTOS A LA ACR-SE Y SUS CLAVES".

- La Política de Certificados de las Autoridades Certificadoras registradas bajo la ACR-SE, será tan restrictiva o más que la especificada en este documento.
- Comunicar inmediatamente, a los titulares de los certificados emitidos por ésta, el compromiso de su clave privada, pérdida, divulgación, modificación, uso no autorizado, con el fin de revocar y volver a generales el par de claves a cada usuario .

## **14. RESPONSABILIDADES**

### **14.1. RESPONSABILIDADES DE LA ACR-SE**

- La DGNM, como administrador de la ACR-SE, garantiza el cumplimiento de las obligaciones descritas en este documento.
- Cualquier anomalía o incidente producidos entre el momento de la revocación de la clave privada de la ACR-SE y el momento de la notificación de tal acto a las Autoridades Certificadoras subordinadas y posterior revocación de los certificados emitidos es responsabilidad única y exclusiva de ACR-SE.
- Cualquier incidente o responsabilidad nacidos de la clave privada de la ACR-SE que se encuentra comprometida, es responsabilidad única y exclusiva de DGNM.

### **14.2. RESPONSABILIDADES DE LA RA-SE.**

- Es responsabilidad de la AR-SE la correcta identificación de los solicitantes, para la emisión de certificados ó para la revocación de los mismos.

### **14.3. RESPONSABILIDADES DE LAS AUTORIDADES CERTIFICADORAS ACREDITADAS POR LA ACR-SE**

- Cualquier anomalía o incidente producidos entre el momento de la revocación, de un certificado emitido por la ACR-SE, y el momento de la notificación de tal evento a la Autoridad de Certificadora, es responsabilidad de ésta última.
- Cualquier incidente o responsabilidad derivados del compromiso de la clave privada de la Autoridad Certificadora subordinada es responsabilidad de ésta.
- Los PSC deberán cumplir con el marco jurídico en lo referente a las responsabilidades de PSC conformado por el CoCo, RPSC y RGPSC.

## **15. REVOCACIONES**

### **15.1. CAUSAS DE REVOCACIÓN**

Cualquier certificado podrá ser revocado si:

- Ha existido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado.
- Se han incumplido alguna de las obligaciones descritas en la Política de Certificados.
- • Se conoce o se tienen motivos para creer razonablemente que uno de

- los hechos representados en el certificado es falso.
- Se conoce que alguno de los requisitos de emisión del certificado no fue cumplido.
- El sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del certificado.
- Fallecimiento del titular del certificado.
- Cambio de información relativa al suscriptor.
- Se sospecha que la información contenida en el certificado es inexacta.
- Resolución administrativa o judicial que lo ordene.
- Se produce un error en la emisión de un certificado.
- Cese voluntario, en el caso de los PSC deberán cumplir con lo establecido en la regla 10 de la RGPSC.
- La clave privada de la ACR-SE fuese comprometida, en cuyo caso, serían revocados todos los certificados de las Autoridades Certificadoras y éstas no podrían emitir certificados válidos hasta que no se restaure la identidad de la ACR-SE y se vuelvan a generar los certificados de las Autoridades Certificadoras registradas por la ACARSE.
- Además de cualquiera de las causas que se señalan en el CoCo, RPSC y RGPSC, que le sean aplicables.

#### **15.2.REVOCACIÓN DE UN CERTIFICADO DIGITAL.**

- La revocación de un certificado digital firmado por la ACR-SE, se realizará siguiendo el procedimiento descrito a continuación:
  - En caso de ser un PSC, será el representante legal del PSC y el profesional informático de la Autoridad Certificadora Subordinada, quienes solicitarán a la ACR-SE la revocación de su certificado.
  - o Para que dicha revocación se lleve a cabo, los responsables deberán cumplir con lo establecido en el artículo 16 del RPSC, anexando los documentos que fundamenten dicha solicitud.
  - o En su caso deberá entregar la documentación que recibieron de los titulares de cada certificado que emitieron.
- En caso de ser una institución pública gubernamental será mediante oficio firmado por el titular y el representante de la institución.
- En caso de un certificado de identidad personal emitidos al personal de la SE o a los particulares que realizan tramites ante la SE, serán éstos los que soliciten la revocación mediante escrito dirigido al Director General de Normatividad Mercantil.

## **ANEXO I. Procedimiento de emisión de Certificados Digitales de Autoridad Certificadora.**

La emisión de un certificado digital firmado por la ACR-SE se hará bajo el procedimiento descrito a continuación:

1 El PSC, deberá designar al profesional informático y responsable directo de la Autoridad Certificadora; Las Instituciones Públicas Gubernamentales designarán al titular del área responsable que emitirá sus certificados; el cual deberá mantener una relación permanente con la ACR-SE.

2 El PSC deberá presentar su documento mediante el cual fue acreditado por la DGNM de conformidad con lo requerido en el trámite SE-09-026-B. Para la identificación fehaciente del titular del certificado, se requerirá su presencia física y deberá presentar una identificación oficial vigente como el pasaporte, credencial del IFE o cedula profesional.

3 La DGNM remitirá dicha información a la ACR-SE, la cual analizará la información requerida en el punto anterior, para determinar si procede o no la emisión del certificado.

4 Estas solicitudes quedarán en poder del ACR-SE. Es responsabilidad de la ACR-SE comprobar que dichas solicitudes están debidamente requisitadas y que todos los datos que aparecen en las mismas son correctos.

5 Confirmada la autenticidad y validez del o los documentos presentados por el PSC, la ACR-SE verificará la razonable coincidencia entre la fotografía contenida en aquellas y la apariencia física del solicitante.

6 La ACR-SE requerirá a las Autoridades Certificadoras subordinadas que firme original y copia del documento de solicitud para verificar la firma autógrafa del documento de solicitud con la que aparece en las credenciales oficiales presentadas, después de lo cual procederá también a la firma autógrafa de la solicitud, considerada a partir de ese momento como aceptada.

7. La ACR-SE, emitirá el certificado correspondiente con el precertificado que presentarán las Autoridades Certificadoras Subordinadas de las siguientes formas:

a. Las Autoridades Certificadoras Subordinadas se autocertificarán su AC, en el nivel más seguro de sus instalaciones, dicho certificado será presentado en un medio de almacenamiento removible, el cual será certificado por la ACR-SE.

b. Las Autoridades Certificadoras Subordinadas emitirán su precertificado en PKCS#10 en su AC, en el nivel más seguro de sus instalaciones, dicho certificado será presentado en un medio de almacenamiento removible, el cual será certificado por la ACR-SE.

Nota: En la **Declaración de Prácticas de Certificación** se detallan los procedimientos correspondientes.