CIRCULAR-TELEFAX 6/2005

México, D.F., a 15 de marzo de 2005.

A LAS INSTITUCIONES
DE CRÉDITO DEL PAÍS:

ASUNTO: INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD (IES).

El Banco de México, con fundamento en lo previsto en los artículos 3° fracción I y 24 de su Ley, y considerando que:

a) Con el objeto de dar mayor seguridad y confianza a las operaciones financieras que se realizan a través de medios electrónicos en los sistemas de pagos, este Instituto Central implementó la "Infraestructura Extendida de Seguridad" (IES) cuya función principal es mantener el control sobre las claves públicas que se utilizan en la verificación de las Firmas Electrónicas, mediante la expedición y administración de Certificados Digitales;

b) Mediante la Circular-Telefax 19/2002 de fecha 5 de julio de 2002 y sus modificaciones, Banco de México, en su carácter de Agencia Registradora Central de la IES, resolvió autorizar a las instituciones de crédito y a las demás instituciones financieras y empresas que les presten a éstas últimas o a las propias instituciones de crédito servicios auxiliares o complementarios relacionados con transferencias de fondos o valores que lo soliciten, para actuar como Agencias Registradoras (AR) y/o Agencias Certificadoras (AC) en la IES, y

c) Resulta conveniente establecer requisitos técnicos e informáticos mínimos, con que deben cumplir los programas de las instituciones de crédito y demás sociedades interesadas en actuar como AR y/o AC en la IES y precisar algunas de las características que deben contener los Certificados Digitales y los requerimientos de tales Certificados.

Ha resuelto emitir las siguientes:

REGLAS PARA OPERAR COMO AGENCIA REGISTRADORA Y/O AGENCIA CERTIFICADORA EN LA INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD

I. Definiciones.

Para los efectos de estas Reglas, en singular o plural se entenderá por:

Agencia Certificadora (AC)	A la institución o empresa autorizada por Banco de México para prestar servicios de certificación en la IES mediante la expedición de Certificados Digitales.
Agencia Registradora (AR)	A la institución o empresa autorizada por Banco de México para llevar el registro electrónico de los Certificados Digitales expedidos por las AC's.
Agencia Registradora Central (ARC)	A Banco de México en su carácter de administrador de la IES que, entre otras funciones, establece las normas de operación de dicha infraestructura, emite, registra y en su caso, revoca los Certificados Digitales de AC y AR, y lleva el registro de las claves públicas.
Agentes Certificadores	A las personas físicas que designe la AC para auxiliarla en el cumplimiento de sus obligaciones en los términos de las presentes Reglas.
Certificado Digital	Al Mensaje de Datos firmado electrónicamente por la AC que lo haya emitido, que confirma el vínculo entre la identidad del Titular con los respectivos Datos de Verificación de Firma Electrónica.
Datos de Creación de Firma Electrónica	A la información única conformada por una clave privada de criptografía asimétrica que el Titular genera bajo su total control y utiliza personalmente para crear una Firma Electrónica.
Datos de Verificación de Firma Electrónica	A la información única conformada por una clave pública de criptografía asimétrica que el Titular genera bajo su total control que está relacionada matemáticamente con los Datos de Creación de Firma Electrónica y que es

	utilizada para comprobar Mensajes de Datos firmados electrónicamente.
Dispositivo de Creación de Firma Electrónica	Al programa y equipo de cómputo que sirve para aplicar los Datos de Creación de Firma Electrónica a un Mensaje de Datos y generar la Firma Electrónica del referido Mensaje de Datos.
Dispositivo de Verificación de Firma Electrónica	Al programa y equipo de cómputo que sirve para aplicar los Datos de Verificación de Firma Electrónica a la Firma Electrónica de un Mensaje de Datos y comprobar su autenticidad.
Firma Electrónica	Al conjunto de datos que se agrega o adjunta a un Mensaje de Datos, el cual está asociado en forma lógica a éste y es atribuible al Titular una vez utilizado el Dispositivo de Verificación de Firma Electrónica.
Infraestructura Extendida de Seguridad (IES)	Al sistema diseñado por Banco de México mediante el cual se administran Certificados Digitales, cuyo propósito es fortalecer la seguridad de la información que se transmite en los sistemas de pagos y atribuir al remitente la autoría de Mensajes de Datos, mediante el uso de Firmas Electrónicas y Certificados Digitales.
Mensaje de Datos	A la información generada, enviada, recibida, archivada y/o comunicada a través de medios electrónicos u otras tecnologías.
Titular	A la persona que genera los Datos de Creación de su Firma Electrónica y los utiliza bajo su exclusivo control, los cuales están matemáticamente relacionados con los Datos de Verificación de Firma Electrónica que constan en su Certificado Digital.

Para efectos de estas Reglas se entenderá por criptografía asimétrica, clave privada y clave pública, lo señalado en la documentación general de la IES que se encuentra a disposición de los interesados en la página que el Banco de México tiene en la red mundial (Internet) que se identifica con el nombre de dominio: www.banxico.org.mx.

II. Requisitos.

Las instituciones de crédito y las instituciones financieras y empresas que les presten a éstas últimas o a las propias instituciones de crédito servicios auxiliares o complementarios relacionados con transferencias de fondos o valores que estén interesadas en actuar como AR y/o AC en la IES, deberán presentar a la Dirección de Trámite Operativo de Banco de México la solicitud de autorización respectiva, en términos del modelo que se adjunta como Anexo 1. Por el sólo hecho de presentar dicha comunicación, las referidas instituciones y empresas manifiestan su conformidad en que les será aplicable lo previsto en las presentes Reglas, en el documento que se refiere el párrafo siguiente y en la demás documentación relacionada con la IES.

El documento que contiene la descripción de las características y funciones de los participantes de la IES, los manuales para el uso de dicha Infraestructura, los Certificados Digitales de la ARC, AR y AC de Banco de México, así como los Certificados Digitales de las empresas o instituciones que hayan obtenido autorización para actuar como AC y/o AR en la IES y el directorio para la atención de consultas, se encuentran a disposición de los interesados en la página que el Banco de México tiene en la red mundial (Internet). Los documentos de referencia están sujetos a actualizaciones periódicas, por lo que será responsabilidad de las instituciones y empresas realizar su consulta de manera frecuente.

Asimismo, las instituciones y empresas solicitantes deberán demostrar al Banco de México, con información que a su juicio resulte suficiente, la fiabilidad de los servicios que prestarán y comprobar que tienen la capacidad tecnológica y el personal calificado para realizar adecuadamente las actividades necesarias en el ámbito de la Firma Electrónica y de la IES. Para tal efecto, deberán cumplir con los requerimientos técnicos e informáticos mínimos para los programas y equipos de cómputo que les permitan interactuar de manera adecuada en la IES, que se establecen en el Anexo 2 de las presentes Reglas.

Con el objeto de que en la citada Infraestructura exista un grado adecuado de seguridad, calidad y confianza en la prestación de servicios de identificación de personas, así como de emisión y registro de Certificados Digitales, las instituciones y empresas deberán presentar para su aprobación las reglas y procedimientos a que se refiere el numeral 1. de los apartados III y IV, según corresponda al tipo de agencia respecto de la que soliciten autorización para actuar, así como, asegurar que podrán cumplir con las demás obligaciones que se señalan en dichos apartados.

Las instituciones y empresas que obtengan autorización para actuar como AC y/o AR en la IES, deberán celebrar con el Banco de México el contrato respectivo y tramitar el Certificado Digital de AC o AR, según corresponda, a fin de estar en posibilidad de emitir o registrar Certificados

Digitales a sus clientes según se trate. Para tal efecto, deberán presentar a la Subgerencia de Instrumentación de Operaciones Nacionales de Banco de México copia certificada y simple, para cotejo, de la escritura en la que consten las facultades para ejercer actos de administración, tanto de la(s) persona(s) que pretendan suscribir el contrato, como de la(s) persona(s) a favor de quien(es) se emitirá(n) los Certificados Digitales de AC y/o AR, así como copia simple de su(s) identificación(es) oficial(es).

III. Obligaciones de la Agencia Certificadora.

1. Contar con reglas y procedimientos sobre prácticas para corroborar la identidad de los solicitantes de Certificados Digitales que sean objetivas, precisas y no discriminatorias.

2. Proporcionar al solicitante de un Certificado Digital el software necesario para que esté en posibilidad de generar, en forma secreta y bajo su total control, sus Datos de Creación de Firma Electrónica y Datos de Verificación de Firma Electrónica. Además, poner a su disposición el software relativo al Dispositivo de Creación de Firma Electrónica y el Dispositivo de Verificación de Firma Electrónica.

3. Requerir para la identificación del solicitante de un Certificado Digital, su comparecencia personal y directa, así como la presentación de su credencial de elector, pasaporte vigente o cualquier otra identificación oficial.

4. Hacer del conocimiento del solicitante, los derechos y obligaciones que adquirirá como Titular de un Certificado Digital, conforme a lo señalado en el apartado V de estas Reglas.

5. Generar Certificados Digitales con base en requerimientos que cumplan con lo dispuesto en el Anexo 3 de las presentes Reglas, así como asegurarse de que tales Certificados Digitales cumplan al menos con las características previstas en el Anexo 4 de dichas Reglas.

6. Obtener la declaración con firma autógrafa del Titular, en términos del modelo que se adjunta como Anexo 5 de estas Reglas, en la que manifiesta su conformidad con las condiciones siguientes: i) ser responsable del uso de su Firma Electrónica, toda vez que cualquier Mensaje de Datos firmado que se pueda comprobar con sus Datos de Verificación de Firma Electrónica le será atribuible y producirá los mismos efectos que las leyes otorgan a los documentos suscritos con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio, y ii) aceptar las condiciones de operación y los límites de responsabilidad de la AC, AR y ARC.

7. Solicitar ante una AR el registro de los Certificados Digitales que emita, así como, en su caso, solicitarle la revocación de éstos inmediatamente después de tener conocimiento de cualquiera de los supuestos previstos en el numeral 3 del Anexo 4 de estas Reglas.

8. Conservar al menos durante 10 años los requerimientos que los solicitantes formulen a la AC para la obtención de Certificados Digitales, realizando las acciones necesarias para impedir que se altere su contenido. Una vez que entre en vigor la "Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos", publicada en el Diario Oficial de la Federación el 4 de junio de 2002, dicha conservación deberá efectuarse de conformidad con la referida Norma.

9. Conservar copia de la información y documentación proporcionada por el Titular para su identificación, así como de la declaración a que se refiere el numeral 6 del presente apartado, por un plazo de al menos 10 años contados a partir de la emisión del correspondiente Certificado Digital, así como abstenerse de utilizar dicha información y documentación para fines diferentes a los relacionados con la IES.

10. Publicar y mantener actualizados en su página en la red mundial (Internet) las disposiciones que emita Banco de México en relación con la Firma Electrónica y la IES, así como las reglas y los procedimientos previstos en el numeral 1 de este apartado III y los Certificados Digitales de AC otorgados a su favor por Banco de México.

11. Proporcionar a Banco de México, en su carácter de ARC de la IES, la información que éste le requiera en relación con sus actividades de certificación y permitir el acceso a sus instalaciones a las personas autorizadas por el propio Banco de México, a fin de que pueda corroborar el cumplimiento de los requisitos previstos en las presentes Reglas, incluyendo la revisión de la seguridad física y lógica de su infraestructura de cómputo.

12. Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasione por negligencia en los procesos de identificación del solicitante, emisión de Certificados Digitales y, cuando así proceda, de la revocación de dichos Certificados. En todo caso, corresponderá a la AC demostrar que actuó con el debido cuidado.

13. Informar a los Titulares de la revocación de su Certificado Digital en la fecha en que ésta se lleve a cabo, cuando dicha revocación se deba a cualquiera de los últimos tres supuestos previstos en el numeral 3.2 del Anexo 4 de estas Reglas.

14. Contar con al menos un respaldo de la información referida en los incisos 8 y 9.

15. Solicitar a la Dirección de Trámite Operativo de Banco de México con una antelación no menor a 60 días naturales, la revocación de la autorización que éste le haya otorgado, cuando pretenda dejar de prestar servicios como AC. En dicha solicitud deberá señalar el nombre de la AC a quien vaya a transferir la información y documentación referida en los numerales 8, 9 y 14 de este apartado. Asimismo, a más tardar el tercer día hábil bancario siguiente a la presentación de la mencionada solicitud, deberá hacer del conocimiento de los Titulares cuyos Certificados Digitales haya emitido, su intención de dejar de actuar como AC y el destino que pretende dar a los datos y documentos de identificación que recibió de ellos.

    En el evento de que la AC que solicite la revocación de la autorización en los términos mencionados sea la única autorizada por Banco de México para desempeñar dichas funciones o bien, que por cualquier circunstancia no le sea posible transferir la referida base de datos a otra AC, deberá transferir a Banco de México, en su carácter de ARC, la información y documentación señalada, en la forma y términos que éste último le indique.

La AC podrá auxiliarse de Agentes Certificadores en el desempeño de las obligaciones previstas en los numerales 2., 3., 4., 6., 8., 9., 13. y 14., así como, para hacer del conocimiento de los Titulares cuyos Certificados Digitales haya emitido, su intención de dejar de actuar como AC y el destino que pretende dar a los datos y documentos de identificación que recibió de ellos, según se prevé en el numeral 15. de este apartado. La AC responderá directamente por los daños y perjuicios que se generen por los actos que realicen los Agentes Certificadores en el cumplimiento de sus funciones.

La AC otorgará Certificados Digitales a sus Agentes Certificadores con el propósito de que el intercambio de información y documentación entre la AC y los referidos Agentes Certificadores, se realice utilizando su Firma Electrónica, a fin de que ambas partes puedan verificar la fiabilidad de dicha información y documentación.

IV. Obligaciones de la Agencia Registradora.

1. Contar con reglas y procedimientos de operación que sean objetivos, precisos y aseguren que los sistemas, las bases de datos y los equipos y programas de cómputo estarán protegidos contra accesos y modificaciones no autorizados, revelaciones indebidas y/o pérdidas de información.

2. Mantener y administrar en línea un registro público de Certificados Digitales en el que quede constancia de la fecha y hora de su emisión, periodo de vigencia y, en su caso, fecha y hora de revocación. Asimismo, deberá conservar los datos de los Certificados Digitales por lo

menos durante 10 años desde su emisión realizando las acciones necesarias para impedir que se altere su contenido. Una vez que entre en vigor la "Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos", publicada en el Diario Oficial de la Federación el 4 de junio de 2002, dicha conservación deberá efectuarse de conformidad con la referida Norma.

3. Permitir la realización de consultas en línea por medios electrónicos al registro público de Certificados Digitales que administre, de conformidad con las especificaciones que para tal efecto determine Banco de México.

4. Contar con mecanismos informáticos y controles que impidan que sus usuarios realicen búsquedas sistemáticas de Certificados Digitales en el registro público mencionado en el numeral 2 anterior.

5. Publicar y mantener actualizados en su página en la red mundial (Internet) las disposiciones que emita Banco de México en relación con la Firma Electrónica y la IES, así como las generalidades de las reglas y los procedimientos previstos en el numeral 1 de este apartado IV y los Certificados Digitales de AR otorgados a su favor por Banco de México.

6. Proporcionar a Banco de México, en su carácter de ARC, la información que éste le requiera en relación con sus actividades de registro y permitir el acceso a sus instalaciones a las personas autorizadas por el propio Banco de México, a fin de que pueda corroborar el cumplimiento de los requisitos previstos en las presentes Reglas, incluyendo la revisión de la seguridad física y lógica de su infraestructura de cómputo.

7. Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasione por negligencia en el proceso de registro o revocación de Certificados Digitales. En todo caso, corresponderá a la AR demostrar que se actuó con el debido cuidado.

8. Contar con al menos un respaldo electrónico de la base de datos de los Certificados Digitales que administra.

9. Revocar Certificados Digitales a solicitud del Titular o de la AC que corresponda, así como cuando la AR tenga conocimiento de que los Datos de Verificación de Firma Electrónica del Titular se han duplicado, o por cualquier razón se encuentre comprometida la integridad o confidencialidad de los Datos de Creación de Firma Electrónica correspondientes. En este último supuesto el procedimiento para dejar sin efecto los Certificados Digitales deberá realizarse en línea, a fin de evitar duplicidad en la IES de los Datos de Verificación de Firma Electrónica respectivos**.** Lo anterior en el entendido de que en todos los casos la AR deberá informar a la AC que haya emitido los Certificados Digitales respectivos, sobre su revocación.

10. Solicitar a la Dirección de Trámite Operativo de Banco de México con una antelación no menor a 60 días naturales, la revocación de la autorización que éste le haya otorgado, cuando pretenda dejar de prestar servicios como AR. En dicha solicitud deberá comunicar el nombre de la AR a quién vaya a transferir la base de datos del registro público de Certificados Digitales que mantiene y administra, así como el correspondiente respaldo electrónico.

    En el evento de que la AR de que se trate sea la única autorizada con tal carácter en la IES, o bien, que por cualquier circunstancia no le sea posible transferir la referida base de datos a otra AR, deberá transmitir a Banco de México, en su carácter de ARC, la citada base de datos de los Certificados Digitales, en la forma y términos que ésta le indique, dentro de los 3 días hábiles siguientes a la fecha en que haya revocado el último Certificado Digital. Asimismo, deberá proporcionarle la demás información que el Banco de México, en su aludido carácter, le requiera.

    En cualquiera de los supuestos antes señalados, la AR de que se trate, dentro de los 3 días hábiles siguientes a la presentación de la solicitud de revocación del Certificado Digital de AR, deberá notificar a los Titulares cuyos Certificados Digitales administra, su intención de dejar de actuar como AR, así como, en su caso, la fecha en que revocará tales Certificados Digitales. La fecha de dichas revocaciones no podrá ser inferior a 15 ni superior a 20 días hábiles contados a partir de la fecha en que haya hecho la notificación a los aludidos Titulares.

V. Derechos y obligaciones de los Titulares.

1. El Titular tendrá los derechos siguientes:

1.1 Ser informado por la AC al menos de:

1.1.1 Las reglas sobre las prácticas para corroborar la identidad, los procedimientos que se seguirán en la prestación del servicio y los elementos técnicos que se utilizarán para brindar seguridad y confidencialidad a la información que proporcione para acreditar su identidad;

1.1.2 Las tarifas de los servicios de certificación;

1.1.3 Los procedimientos para la utilización del Certificado Digital y, en su caso, sus limitaciones de uso, así como de las posibles implicaciones que conlleve que terceros

conozcan sus Datos de Creación de Firma Electrónica o la frase de seguridad vinculada con ellos;

1.1.4 Las características generales de los procedimientos de creación y verificación de Firmas Electrónicas;

1.1.5 Los procedimientos para dirimir controversias, así como la ley aplicable y los tribunales competentes;

1.1.6 Los medios que puede utilizar para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar reclamaciones;

1.1.7 Los límites de las responsabilidades de la AC, AR y ARC, y

1.1.8 La revocación de su Certificado Digital y la causa de dicha revocación, cuando ésta se deba a cualquiera de los últimos tres supuestos previstos en el numeral 3.2 del Anexo 4 de estas Reglas.

1.2 Recibir de la AC el software necesario para que esté en posibilidad de generar en secreto y en forma individual sus Datos de Creación de Firma Electrónica y sus Datos de Verificación de Firma Electrónica.

1.3 Mantener en secreto sus Datos de Creación de Firma Electrónica.

1.4 Tener acceso a un servicio que le permita, en todo momento, revocar en línea su Certificado Digital.

1.5 Tener acceso a un servicio en línea, que en todo momento, le permita verificar el estado de cualquier Certificado Digital que le interese.

1.6 Ser informado por la AR de la revocación de su Certificado Digital en el supuesto previsto en el numeral 10 del Apartado IV anterior.

2. El Titular tendrá las obligaciones siguientes:

2.1 Hacer declaraciones veraces y completas en relación con los datos y documentos que proporcione para su identificación personal.

2.2 Firmar la carta de aceptación respectiva, antes de recibir su Certificado Digital.

2.3 Dar aviso a la AC de cualquier modificación de los datos a que se refiere el numeral anterior inmediatamente después de que éstos cambien.

2.4 Custodiar adecuadamente sus Datos de Creación de Firma Electrónica y la frase de seguridad vinculada con ellos, a fin de mantenerlos en secreto.

2.5 Solicitar inmediatamente a la AC que realice los trámites necesarios ante la AR o bien, solicitar directamente a esta última, la revocación de su Certificado Digital, en caso de que la integridad y/o confidencialidad de sus Datos de Creación de Firma Electrónica hayan sido comprometidas.

VI. Límites de responsabilidad de la Agencia Registradora Central.

La ARC no responderá por los daños y/o perjuicios que se causen, directa o indirectamente, por la utilización que se realice o pretenda realizarse de la IES, incluyendo los que se causen con motivo de la emisión, registro y revocación de Certificados Digitales.

TRANSITORIOS

PRIMERO.- La presente Circular-Telefax entrará en vigor el 16 de marzo de 2005.

SEGUNDO.- A partir de la entrada en vigor de la presente Circular-Telefax queda abrogada la Circular-Telefax 19/2002 emitida por el Banco de México el 5 de julio de 2002, así como sus modificaciones.

ANEXO 1

MODELO DE COMUNICACIÓN PARA SER ENVIADA POR LAS INSTITUCIONES Y EMPRESAS QUE SOLICITEN AUTORIZACIÓN DEL BANCO DE MÉXICO PARA ACTUAR COMO AGENCIA CERTIFICADORA Y/O AGENCIA REGISTRADORA, ASÍ COMO PARA QUE SE EXPIDAN LOS CERTIFICADOS DIGITALES RESPECTIVOS

(*MEMBRETE DE LA INSTITUCIÓN o EMPRESA*)

México, D. F., a ___ de _____de 200_.

BANCO DE MÉXICO
Dirección de Trámite Operativo,

En relación con la Circular-Telefax __/2005 de fecha __ de ____ de 2005, (*Denominación de la institución o empresa*) solicita a Banco de México autorización para actuar como (*Tipo de agencia cuya función pretende realizar*), así como, la expedición del Certificado Digital respectivo a nombre de (*Nombre (del) (de los) apoderado(s) de la institución o empresa para dicho propósito*) a fin de estar en posibilidad de actuar con tal carácter en la IES.

Al efecto, adjunto a la presente sometemos a la consideración de ese Instituto Central la documentación que acredita que (*Denominación o razón social de la institución o empresa*) cumple con los requisitos establecidos en la Circular-Telefax mencionada para actuar como (*Tipo de agencia cuya función pretende realizar*), así como la copia certificada y simple de la escritura pública en la que consta el poder para actos de administración otorgado a la(s) persona(s) señalada(s) en el primer párrafo de la presente comunicación.

Asimismo, esta (*institución o empresa*) se obliga a proporcionar a Banco de México la información adicional que nos requiera en relación con las actividades mencionadas, así como permitir el acceso a nuestras instalaciones al personal autorizado por ese Instituto Central a fin de que puedan corroborar el cumplimiento de los citados requisitos.

A t e n t a m e n t e ,

(*Denominación o razón social de la institución o empresa*)

(Nombre y firma de la(s) persona(s) facultada(s))

(Cargo(s))

ANEXO 2[1]

REQUERIMIENTOS TÉCNICOS E INFORMÁTICOS MÍNIMOS DE LOS PROGRAMAS Y EQUIPOS DE CÓMPUTO QUE PERMITEN INTERACTUAR DE MANERA ADECUADA EN LA INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD

1. Para una Agencia Registradora:

1.1. Deberá utilizar un sistema informático disponible 7x24[2], que opere con un Certificado Digital de AR emitido por la ARC.

1.2. Mantener una conexión permanente[3] con la ARC, con las características y los mensajes del protocolo de comunicaciones que establezca la propia ARC[4].

1.3. La secuencia de mensajes deberá contener al menos:[5]

1.3.1. (AR → ARC) ConnUsr

1.3.2. (ARC → AR) IdUsuarioAleat ó desconexión de la AR

1.3.3. (AR → ARC) IdFmaAleat

1.3.4. (ARC → AR) Logged

.3.5. (AR → ARC) IdAutMsg

.4. Deberá permitir la conexión a clientes propios y externos, mediante un protocolo de comunicaciones seguro especificado por la ARC**,** sin perjuicio del medio de comunicación que utilicen las herramientas propias para la solicitud de los Certificados Digitales[6].

La secuencia de mensajes al menos deberá ser[7]:

---

1 Las referencias a páginas electrónicas en la red mundial (Internet) contenidas en las siguientes notas al pie de página, corresponden a la fecha de emisión de estas Reglas, por lo que, dichas referencias pueden estar sujetas a cambios.

2 Un sistema 7x24 es aquél que está disponible los 7 días de la semana, 24 horas al día.

3 En caso de que dicha conexión se interrumpa, la AR deberá intentar reestablecerla y en tanto no lo haga, se abstendrá de registrar nuevos Certificados Digitales; lo anterior, sin perjuicio de que conserve las revocaciones de los Certificados Digitales que se verifiquen durante dicho período, debiendo mandar éstas a la ARC tan pronto se reestablezca la comunicación.

4 Para mayor información sobre los protocolos de comunicaciones seguros, especificados por la ARC, referirse al documento denominado "Protocolo de comunicación con la IES" de agosto de 2003, y a las actualizaciones y/o modificaciones que, en su caso, realice el Banco de México.

5 Para mensajes de la AR a la ARC, se usará el prefijo (AR → ARC). Para mensajes de respuesta de la ARC se usará el prefijo (ARC → AR).

6 Deberá comunicarse adecuadamente con el sistema WebSecBM.

7 Para mensajes del cliente a la AR, se usará el prefijo (Clnt → AR). Para mensajes de respuesta de la AR al cliente se usará el prefijo (AR → Clnt).

1.4.1. (Clnt → AR) ConnUsr

1.4.2. (AR → Clnt) IdUsuarioAleat

1.4.3. (Clnt → AR) IdFmaAleat

.4.5. (AR → Clnt) Logged

.4.6. (Clnt → AR) PideCrtNvoFmt

.4.7. (AR → Clnt) RegCrtNvoFmt, CrtNoExiste o AutNoConn

.5. Deberá permitir sólo el registro de Certificados Digitales con un número de serie igual a NNNNNNMMMMMMXXXXXXXX, donde tanto NNNNNN (el número de AR) como MMMMMM (el número de AC) son números asignados por la ARC. El número XXXXXXXX será asignado de acuerdo al número de Certificados Digitales emitidos por la AC[8].

.6. Para el registro de Certificados Digitales, deberá recibir confirmación de unicidad de la clave pública por parte de la ARC antes de permitir el registro de un nuevo Certificado Digital. Los mensajes a utilizar, al menos deberán ser los siguientes:

1.6.1. (AR → ARC) AltaCrt

1.6.2. (ARC → AR) CrtAceptado o CrtRechazado

Sólo deberá registrar Certificados Digitales si recibe el mensaje CrtAceptado.

1.7. El envío de Certificados Digitales a la ARC para validar la unicidad de la clave pública deberá hacerse en formato PEM[9].

1.8. Las consultas de Certificados Digitales deberán ser resueltas en primera instancia por la AR receptora de la solicitud. Si el número de AR del Certificado Digital no corresponde con el que la AR receptora tenga asignado, ésta deberá reenviar la solicitud a la ARC o a la AR correspondiente. En caso de que sea a la ARC, podrá hacerlo a través de la conexión permanente mencionada en el numeral 1.2. del presente Anexo, o a través de otra conexión a la ARC previamente autorizada. En caso de que se use una nueva conexión, la secuencia de mensajes deberá ser igual a la descrita en el numeral 1.4. anterior, con la ARC en el rol de AR y la AR actuando como el cliente.

1.9. Los avisos de revocación que reciba de una AC, deberá reenviarlos a la ARC, mediante el mensaje:

1.9.1 (AR → ARC) RevBrdcst

---

[8] La AC asigna los últimos 8 dígitos y la AR deberá revisar que el número de serie completo cumpla con el formato establecido en el presente Anexo 2 y en el Anexo IV de estas Reglas.

[9] El formato PEM es un formato estándar en el que se pueden representar los certificados X509 y permite, entre otras cosas, su transmisión por correo electrónico sin que haya alteraciones en los servidores, ya que es un formato en texto.

1.10 Los avisos de revocación que reciba de la ARC, mediante el mensaje:

1.10.1 (ARC → AR) RevBrdcst

Deberá reenviarlos a sus clientes con un mensaje similar.

2. Para una Agencia Certificadora:

2.1. Deberá ser un sistema informático operado por un empleado de la institución o empresa de que se trate, que cuente con un Certificado Digital de AC emitido por la ARC.

2.2. Deberá conectarse a la AR correspondiente, utilizando un protocolo de comunicaciones seguro, al menos, con el mismo nivel de seguridad que el utilizado entre la AR y la ARC.

2.3. Deberá aceptar requerimientos tanto en PEM como en DER[10], en el formato conocido como PKCS#10[11].

2.4. Deberá reconocer el mensaje de aviso de revocación de la AR, ya sea en un protocolo propio, o en el mismo que utilice la ARC para avisar de la revocación a las AR's.

3. Para Agencia Registradora y Agencia Certificadora:

3.1. Los equipos donde se ejecuten las aplicaciones relacionadas con las funciones de AR y AC, deberán utilizar el protocolo NTP (Network Time Protocol) para sincronizar el reloj del equipo con el Tiempo Universal Coordinado (UTC) o un protocolo equivalente que garantice un nivel de confiabilidad igual o mayor a los que garantiza NTP con respecto al patrón UTC.

[10] El formato DER es la representación binaria del requerimiento.

[11] El formato PKCS#10 establece los campos del requerimiento y está descrito en la página de la red mundial (Internet) que se identifica con el nombre de dominio http://www.rsasecurity.com/rsalabs/node.asp?id=2132.

ANEXO 3[12]

CARACTERÍSTICAS DE LOS REQUERIMIENTOS DE LOS CERTIFICADOS DIGITALES

El formato del requerimiento de un Certificado Digital deberá cumplir con el estándar RSA PKCS#10.

Los requerimientos de los Certificados Digitales tendrán al menos el contenido siguiente:

1. La versión del requerimiento indicada explícitamente.
2. El nombre distinguido que identifica al Titular del requerimiento conteniendo, al menos, los campos siguientes:
   - Nombre del Titular, en el campo commonName (OID[13] 2.5.4.3).
   - En su caso, el Registro Federal de Contribuyentes (RFC) (incluyendo la homoclave) del Titular, en el campo x500UniqueIdentifier (OID 2.5.4.45).
   - En su caso, el domicilio del Titular, en el campo direcciónPostal (OID 2.37.1117.1973.19) o en el campo postalAddress (OID 2.5.4.16).
   - En su caso, la dirección de correo electrónico del Titular, en el campo emailAddress (OID 1.2.840.113549.1.9.1).
3. Los Datos de Verificación de Firma Electrónica.
4. Un atributo conteniendo el challengePassword[14]. El OID del mismo deberá ser el 1.2.840.113549.1.9.7 y se deberá generar de la manera siguiente: Se concatena el RFC del Titular a una frase o palabra clave y en caso que el titular no tenga RFC se usará simplemente la frase o palabra clave elegida por el usuario de manera secreta. A esta cadena aplicarle el

---

12 Las referencias a páginas electrónicas en la red mundial (Internet) contenidas en las siguientes notas al pie de página, corresponden a la fecha de emisión de estas Reglas, por lo que dichas referencias pueden estar sujetas a cambios.

13 OID Object IDentifier – Identificador de Objeto por sus siglas en inglés. La definición formal se encuentra en la recomendación X.208 (ASN.1) de la ITU- T, disponible en la página de la red mundial (Internet) que se identifica con el nombre de dominio http://www.itu.ch.

14 El atributo “challengePassword” es descrito en forma general en el PKCS#9, publicado en la página de la red mundial (Internet) que se identifica con el nombre de dominio http://www.rsasecurity.com/rsalabs/node.asp?id=2131.

algoritmo de digestión SHA1[15] y después filtrarlo con el algoritmo Base 64[16]. El resultado final será el Challenge Password que deberá incluirse en el requerimiento.

5. La Firma Electrónica generada con la clave privada correspondiente a los Datos de Verificación de Firma Electrónica contenida en el mismo requerimiento, deberá ser almacenada dentro del requerimiento de acuerdo a su estándar.

[15] El algoritmo SHA1 (Secure Hash Algoritm One) está descrito en el RFC 3174 "US Secure Hash Algorithm 1 (SHA1)", disponible en la página de la red mundial (Internet) que se identifica con el nombre de dominio (URL): ftp://ftp.rfc-editor.org/in-notes/rfc3174.txt.

[16] El algoritmo Base 64 está descrito en el RFC 3548 "The Base16, Base32, and Base64 Data Encodings", disponible en la página de la red mundial (Internet) que se identifica con el nombre de dominio (URL): ftp://ftp.rfc-editor.org/in-notes/rfc3548.txt.

ANEXO 4

CARACTERÍSTICAS DE LOS CERTIFICADOS DIGITALES.

1. El formato del Certificado Digital deberá apegarse a la especificación ITU-T X.509v3.

2. Los Certificados Digitales deberán contar, al menos, con el contenido siguiente:

   2.1 La indicación de que se trata de un Certificado Digital.

   2.2 Un código de identificación único del Certificado Digital de 20 dígitos, organizados de izquierda a derecha de la manera siguiente:

      2.2.1 Primeros 6 dígitos (posiciones de la 1 a la 6), para identificar a la AR que tiene almacenado el Certificado Digital. Este número es asignado por Banco de México en su carácter de ARC.

      2.2.2 Segundos 6 dígitos (posiciones de la 7 a la 12), para identificar a la AC que expidió el Certificado Digital. Este número es asignado por Banco de México en su carácter de ARC.

      2.2.3 Últimos 8 dígitos (posiciones de la 13 a la 20), número consecutivo del Certificado Digital asignado por la AC que lo emita.

   2.3 Identificación de la AC que emite el Certificado Digital con indicación de su nombre o razón social y dirección de correo electrónico, así como su Firma Electrónica.

   2.4 Datos de identificación del Titular, entre los cuales deben necesariamente incluirse el nombre y los Datos de Verificación de Firma Electrónica.

   2.5 La fecha y hora de inicio y fin del periodo de validez del Certificado Digital.

   2.6 Opcionalmente, podrán contener los datos de verificación de la firma EDIFACT.

3. Los Certificados Digitales quedarán sin efecto en los casos siguientes:

   3.1 Por extinción del periodo de validez del propio Certificado Digital, el cual no podrá exceder de dos años contados desde la fecha de su emisión.

3.2 Por revocación en las circunstancias siguientes:

3.2.1 A solicitud del Titular;

3.2.2 Por fallecimiento del Titular;

3.2.3 Por resolución judicial;

3.2.4 Cuando la AC, la AR o la ARC tengan conocimiento de que el Titular incumplió sus obligaciones en relación con la IES.

3.2.5 Al comprobar la ARC, la AC o la AR que existe una solicitud de registro de un Certificado Digital que, de ser aceptada, implicaría la duplicidad de los Datos de Verificación de Firma Electrónica de un Titular en la IES, o por cualquier razón se encuentre comprometida la integridad o confidencialidad de los Datos de Creación de Firma Electrónica o la frase de seguridad vinculada a ellos. En este supuesto, el procedimiento para dejar sin efecto el Certificado Digital deberá realizarse en línea para evitar duplicidad de los Datos de Verificación respectivos, dentro de la IES.

En caso de que la referida comprobación se lleve a cabo por la ARC, ésta deberá informarle tal situación a la AC que haya emitido el Certificado Digital correspondiente y ordenar de inmediato la revocación del Certificado Digital a la AR que lo haya registrado. El procedimiento de revocación de los Certificados Digitales deberá llevarse a cabo en línea.

3.3 Por revocación de la autorización otorgada por Banco de México a la AR o cuando deje de tener el carácter de institución financiera, prestar los servicios de banca y crédito, o bien los servicios auxiliares o complementarios relacionados con transferencias de fondos o valores, según corresponda.

ANEXO 5

MODELO DE CARTA DE ACEPTACIÓN EN LA QUE DEBERÁ CONSTAR LA FIRMA AUTÓGRAFA DEL TITULAR DE UN CERTIFICADO DIGITAL

México, D. F., a ___ de _____de 200__.

El suscrito (Usuario), para todos los efectos legales a que haya lugar, manifiesta haber solicitado a (*Denominación o razón social de la institución o empresa*) en su carácter de Agencia Certificadora, la emisión de un Certificado Digital en el que consten los Datos de Verificación de Firma Electrónica (clave pública) asociados a los Datos de Creación de Firma Electrónica (clave privada) y frase de seguridad, que generó previamente en absoluto secreto. Asimismo, afirma haber manifestado su conformidad en que la Agencia Certificadora utilizara el procedimiento descrito en sus reglas de operación.

El Usuario reconoce que para la emisión del referido Certificado Digital, la Agencia Certificadora únicamente revisó la identificación oficial con fotografía, mediante la cual el propio Usuario se identificó, constatando a simple vista que dicho documento corresponde con sus rasgos fisonómicos y caligráficos, por lo que el Usuario asume responsabilidad exclusiva respecto de la autenticidad de tal documento, así como, de la veracidad de los demás datos que haya proporcionado a la Agencia Certificadora en el proceso de su identificación.

El Usuario en este acto, acepta el Certificado Digital cuya clave pública consta al final del presente documento, sirviendo éste último, como el recibo más amplio que en derecho proceda.

Adicionalmente, el Usuario acepta que el uso de la clave privada y frase de seguridad con base en los cuales dicho Certificado Digital fue elaborado, quedarán bajo su exclusiva responsabilidad. Por lo anterior, se obliga a mantener absoluta confidencialidad respecto de las aludidas clave privada y frase de seguridad, así como a realizar los trámites necesarios para solicitar la revocación de dicho Certificado Digital ante la Agencia Certificadora, mediante los mecanismos y en los horarios que la misma establezca, en el evento de que por cualquier causa dicha información haya sido divulgada y, por tanto, la integridad y/o confidencialidad de dicha información haya sido comprometida.

Por otra parte, el Usuario reconoce y acepta que la Agencia Certificadora y la Agencia Registradora únicamente serán responsables por los daños y perjuicios que le llegaren a causar, derivados de errores que, en su caso, cometan por negligencia en el proceso de generación, registro, entrega y revocación del Certificado Digital, así como, que no serán responsables por los daños y perjuicios

que se pudieran causar al Usuario o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho Certificado Digital.

De la misma forma, el Usuario reconoce y acepta que Banco de México, en su carácter de Agencia Registradora Central no responderá por los daños y/o perjuicios que se causen, directa o indirectamente, por la utilización que se realice o pretenda realizarse de la IES, incluyendo los que se causen con motivo de la emisión, registro y revocación de Certificados Digitales.

Datos del Certificado:

Datos de la AC:

Datos del Usuario:

Clave Pública del Usuario:

Firma Electrónica de la AC:

(*Nombre y firma autógrafa del Titular del Certificado Digital*)