Infraestructura Extendida de Seguridad

IES

BANCO DE MÉXICO

Dirección General de Sistemas de Pagos y Riesgos
Dirección de Sistemas de Pagos

INDICE

INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD

1. INTRODUCCION

Con el desarrollo de las nuevas tecnologías de telecomunicaciones y transmisión de datos por vía electrónica, se ha generalizado el uso de los sistemas de intercambio electrónico de información, en virtud, de que permiten mejorar la productividad y reducir costos, además de que brindan amplias posibilidades de nuevos servicios en línea.

Por ello, se hace necesario disponer de un entorno seguro en relación con la autenticación electrónica y en este contexto la firma electrónica es una herramienta esencial para dar seguridad y confianza a las redes de comunicación, ya que cumple con las dos principales características de las firmas autógrafas: atribuir el documento al signatario y verificar que el mensaje no ha sido manipulado después de su firma.

La Infraestructura Extendida de Seguridad (IES) es un sistema diseñado y administrado por Banco de México con el propósito de fortalecer la seguridad de la información que se transmite tanto en los sistemas de pagos como entre el sistema financiero mexicano y el Banco Central.

La IES administra certificados digitales, los cuales son a su vez mensajes de datos firmados digitalmente por una entidad del sistema de administración. La seguridad está basada en el uso de firmas electrónicas mediante la aplicación de algoritmos criptográficos para garantizar la confidencialidad e integridad de la información que se transmite y así acreditar la identidad del remitente.

El objetivo del presente documento es explicar brevemente cuál es la estructura y organización de la IES.

2. LA IES DISEÑADA POR BANCO DE MÉXICO

A fin de proveer una operación segura y eficiente tanto en los sistemas de pagos como en la comunicación a través de mensajes electrónicos protegidos mediante algoritmos de criptografía asimétrica (clave pública y privada), es necesario tener una infraestructura que permita administrar y distribuir las claves públicas en forma ágil y con la confianza de que cada correlación de clave pública y usuario implica

necesariamente la corroboración de la identidad de los usuarios con base en la comparecencia física y presentación de documentación oficial.

2.1 CERTIFICADOS DIGITALES

El control y administración de las claves públicas de los usuarios se realiza a través de la expedición de *certificados digitales*.

Un certificado digital es un documento electrónico que asegura que una clave pública determinada corresponde a un individuo en específico. Dicho certificado está firmado electrónicamente por la agencia que corroboró de manera razonable la identidad del individuo y la validez de su clave pública.

Un certificado digital usualmente contiene un número de identificación del certificado, una clave pública, los datos personales que identifican al propietario de la clave pública, las características propias de la clave, la vigencia del certificado y los datos particulares de la agencia certificadora, así como su firma electrónica.

2.2 FINALIDAD Y FUNCIONES

El objetivo principal de la IES es dar mayor seguridad y confianza a las operaciones financieras que se realizan a través de los medios electrónicos en los sistemas de pagos.

Para la consecución de tal objetivo, la IES tiene como función principal mantener el control sobre las claves públicas que se utilicen en la verificación de las firmas electrónicas, mediante la expedición y administración de certificados digitales.

2.3 ESTRUCTURA DE ORGANIZACIÓN

La estructura de organización de la IES establecida y administrada por Banco de México es flexible en el sentido de que es totalmente independiente del sistema criptográfico que se use. La estructura puede crecer gradualmente de acuerdo a las necesidades de los diferentes usuarios y permite que la administración de las claves quede distribuida entre diversos participantes, estableciendo para ello varios servidores de certificados digitales interconectados para satisfacer en forma ágil los requerimientos de los usuarios.

El modelo general de organización para la administración de las claves públicas y los certificados digitales se muestra en el ANEXO 1 en el que se aprecia que los participantes de la IES son:

- Agencia Registradora Central ARC
- Agencias Registradoras AR's
- Agencias Certificadoras AC's
- Agentes Certificadores AgC's
- Usuarios

2.4 PRINCIPALES FUNCIONES DE LOS PARTICIPANTES

Las principales funciones que desempeñan cada uno de los participantes de la IES se describen a continuación:

ARC – Agencia Registradora Central

- Normar y administrar la IES de acuerdo con las políticas que establezca el Banco de México.
- Crear su propio certificado digital y certificar a las AR's y AC's.
- Garantizar la unicidad de las claves públicas del sistema.
- Administrar la base de datos de las claves públicas correspondientes a los certificados digitales que las AR's tengan registradas en sus bases de datos y mantener una liga con las AC's que los expidieron.
- Difundir su clave pública y las claves públicas de las AR's y AC's a través de 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.
- Establecer, administrar y mantener las medidas que garanticen la seguridad del sistema.

AR's – Agencias Registradoras

- Registrar certificados digitales siempre y cuando la ARC confirme la unicidad de las claves públicas.
- Administrar las bases de datos con los certificados digitales registrados, tanto vigentes como históricas.
- Proporcionar a los usuarios que lo soliciten a través de medios electrónicos, información respecto de certificados digitales.
- Revocar certificados digitales en los supuestos previstos en las disposiciones aplicables e informar de la revocación a la AC que los haya emitido, así como, divulgar dichas revocaciones de conformidad con las reglas emitidas por la ARC.

AC's – Agencias Certificadoras

- Emitir certificados digitales.
- Emitir los certificados digitales de las personas que les presten los servicios de AgC's y acreditarlos como tales.
- Solicitar a la AR que corresponda, la revocación de los certificados digitales que haya emitido, en los supuestos previstos en las disposiciones aplicables o cuando los usuarios, directamente o a través de un AgC, lo soliciten.
- Auxiliarse de AgC's en la realización de sus funciones, de conformidad con las disposiciones aplicables.
- Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasione por negligencia en el proceso de certificación, de conformidad con las disposiciones aplicables.
- Responder por los actos que realicen sus AgC´s, así como de los daños y perjuicios que éstos generen en el cumplimiento de sus funciones, de conformidad con lo previsto en las disposiciones aplicables.

AgC's – Agentes Certificadores

- Auxiliar a la AC en la realización de sus funciones de conformidad con las disposiciones aplicables.
- Verificar la identidad de los solicitantes que desean obtener certificados digitales, con base en los documentos oficiales que éstos les presenten.
- Informar al solicitante de un certificado digital sus derechos y obligaciones.
- Recibir y verificar el requerimiento de certificado digital elaborado por el solicitante.
- Obtener una declaración con firma autógrafa del solicitante en la que manifieste su conformidad con las reglas sobre el uso de firma electrónica.
- Proporcionar al solicitante de un certificado digital los medios necesarios para la generación de datos de creación y verificación de su firma electrónica.
- Emitir el precertificado correspondiente y solicitar el respectivo certificado digital a la AC que corresponda.
- Entregar al titular su certificado digital registrado y obtener la carta de aceptación del referido certificado digital en la que conste su firma autógrafa.
- Informar, en su caso, al titular de la revocación de su certificado digital.

Usuarios

- Solicitar su certificado digital a una AC directamente o a través de un AgC, presentando su requerimiento digital y los documentos oficiales para su identificación, así como en su caso, la carta de solicitud correspondiente.
- Ser informado de sus derechos y obligaciones y manifestar su conformidad con las disposiciones aplicables a la firma electrónica.
- Establecer, en secreto y en forma individual, su frase de seguridad con la que podrá cifrar su clave privada para protegerla.
- Generar, en secreto y en forma individual, su par de claves (pública y privada) y su requerimiento, así como, los archivos correspondientes.
- Recibir la carta de aceptación de su certificado digital en la que conste su firma autógrafa y su certificado digital ya registrado.
- Mantener en un lugar seguro su clave privada.
- Recordar su frase de seguridad así como su Challenge Password y mantenerlos en secreto.
- Solicitar a la AR a través de medios electrónicos, la información de los certificados digitales de aquellos usuarios con los que tiene una relación operativa.
- Tener acceso a un servicio que le permita revocar, en línea, su certificado digital en cualquier momento.
- Ser informado por la AC o, en su caso, por un AgC, de las reglas, procedimientos y características generales de los servicios de certificación y de los certificados digitales.

2.5 ORGANIZACIÓN

La IES está organizada a través de las agencias siguientes:

- La ARC, bajo la responsabilidad exclusiva de Banco de México;
- Las AR y AC's, que están bajo la responsabilidad del propio Instituto Central, y
- La AR's y las AC's de aquellas instituciones y/o empresas que hayan sido autorizadas por Banco de México para actuar con tal carácter en la IES.

La IES opera con un certificado raíz, es decir el de la ARC. Este certificado ampara la validez de los certificados expedidos para las AC's y AR's. Finalmente los certificados de AC's amparan la validez de los certificados de usuarios final.

2.6 SEGURIDAD OPERATIVA

Es interés del Banco de México que la IES opere en un entorno confiable que permita asegurar que la asociación de claves públicas con los participantes del sistema sea fidedigna.

Considerando que la funcionalidad y seguridad de un sistema informático depende de todos y cada uno de sus componentes, se han incorporado a la IES diversos procedimientos de seguridad, esto con el objetivo de garantizar la confiabilidad de la base de datos y la continuidad operativa.

3. USO Y EXPLOTACIÓN DE LA IES

3.1 PROCEDIMIENTO PARA LA OBTENCIÓN DE UN CERTIFICADO DIGITAL.

El procedimiento para la obtención de un certificado digital se deberá llevar a cabo conforme a las prácticas de certificación elaboradas por la AC que corresponda, previamente aprobadas por Banco de México, así como, por lo previsto en las disposiciones aplicables a la IES.

3.2 USO DE FIRMAS ELECTRÓNICAS.

De acuerdo con la definición de firma electrónica, el signatario es una persona física que suscribe documentos utilizando un dispositivo y sus datos de creación de firma, y el destinatario del documento es la persona física que verifica la firma utilizando un dispositivo y los datos de verificación de firma del signatario

Los datos que el signatario utiliza para crear la firma electrónica son, como ya se mencionó, su clave privada, frase de seguridad y certificado digital. Los datos que el destinatario utiliza para verificar la firma electrónica son los del certificado digital del signatario, el cual lo obtiene de la IES a través de una AR.

De este modo el signatario y el destinatario deben contar, respectivamente, con dispositivos de creación y verificación de firmas electrónicas, los cuales deben ser sistemas de cómputo cuya función principal sea la aplicación de algoritmos criptográficos. A su vez, dichos sistemas deben mantener comunicación con la IES, en particular con una AR, para estar en posibilidad de solicitar y verificar la

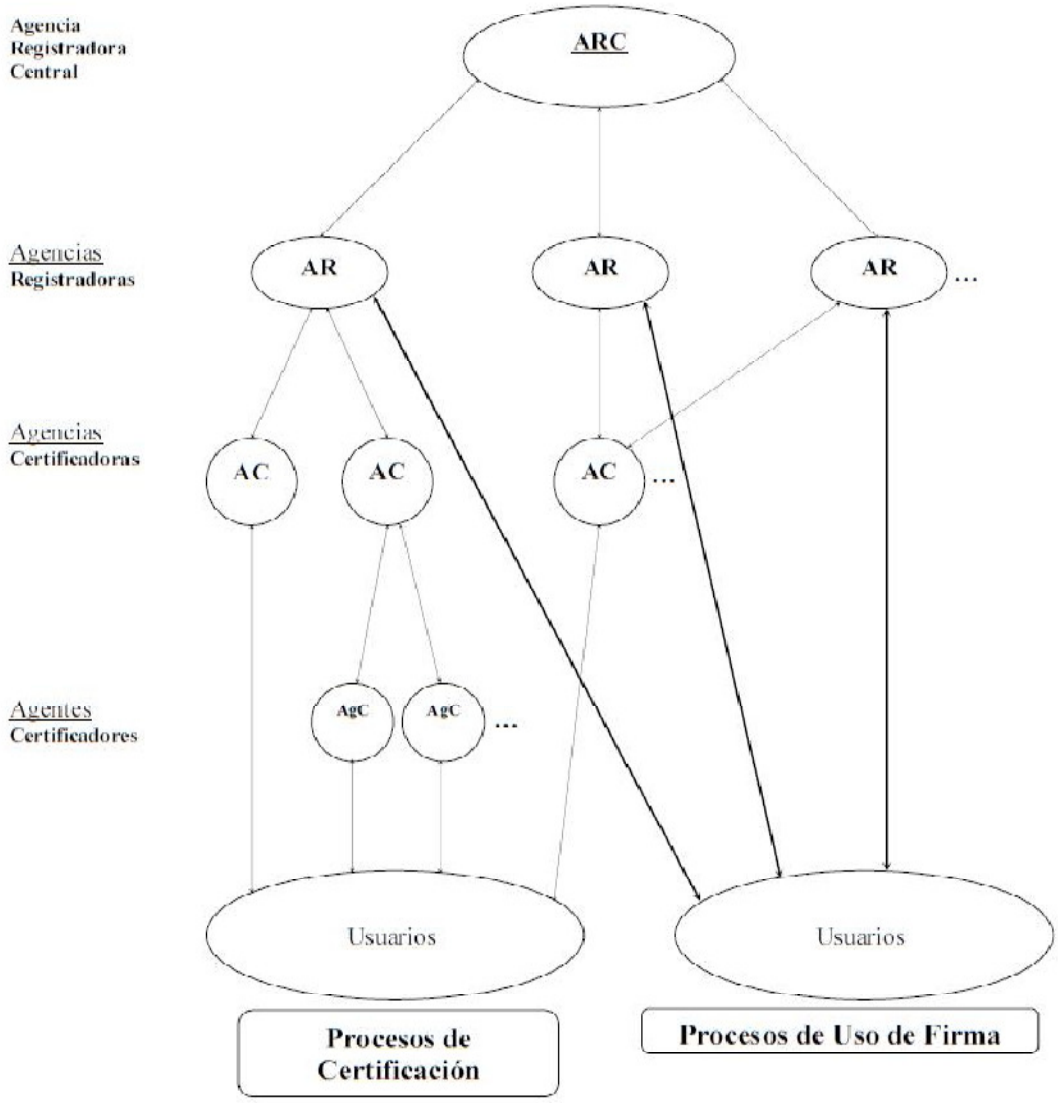
validez de los certificados digitales de los usuarios involucrados en los procesos de firma y cifrado de documentos.

4. ATENCIÓN DE CONSULTAS

Para consultas acerca de aspectos técnicos relacionados con la IES, los interesados podrán enviar un correo electrónico a la dirección electrónica ies@banxico.org.mx.

ANEXO 1 Estructura de la IES

MODELO ORGANIZACIONAL DE LA IES



16