



Política de Certificación de Certificados de Firma Fiable con limitación uso sobre dispositivo seguro (SSCD)

Fecha: 10/07/09 **Versión:** 1.2
Estado: VIGENTE **Nº de páginas:** 36
OID: 1.3.6.1.4.1.30051.2.2.2.1.1 **Clasificación:** PUBLICO
Archivo: ACEDICOM - Politica FirmaAtributosSoft.doc
Preparado por: Autoridad de Certificación EDICOM - ACEDICOM

Historial de cambios			
Versión	Fecha	Descripción de la acción	Páginas /sección
1.0	03/10/08	Documento inicial	
1.1	09/02/09	Modificaciones propuestas por las Secretaria de Economía	
1.2	10/07/09	Cambios menores por erratas	

Tabla de Contenido

1. INTRODUCCIÓN	8
1.1. PRESENTACIÓN	8
1.2. IDENTIFICACIÓN	10
1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN.....	10
1.3.1. Autoridades de Certificación.....	10
1.3.2. Autoridades de Registro	10
1.3.3. Usuarios Finales	10
1.4. USO DE LOS CERTIFICADOS	10
1.4.1. Usos Permitidos.....	10
1.4.2. Usos prohibidos	11
1.4.3. Fiabilidad de la firma electrónica a lo largo del tiempo	11
1.5. POLÍTICA DE ADMINISTRACIÓN	12
1.5.1. Especificación de la Organización Administradora	12
1.5.2. Persona de Contacto	12
1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas	12
1.6. DEFINICIONES Y ACRÓNIMOS.....	12
1.6.1. Definiciones	12
1.6.2. Acrónimos.....	12
2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS..	13
2.1. REPOSITORIO DE CERTIFICADOS	13
2.2. PUBLICACIÓN	13
2.3. FRECUENCIA DE ACTUALIZACIONES	13
2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.	13
3. IDENTIFICACIÓN Y AUTENTICACIÓN	14
3.1. REGISTRO DE NOMBRES	14
3.1.1. Tipos de nombres	14
3.1.2. Significado de los nombres	14
3.1.3. Interpretación de formatos de nombres.....	14
3.1.4. Unicidad de los nombres	14
3.1.5. Resolución de conflictos relativos a nombres	14
3.1.6. Reconocimiento, autenticación y función de las marcas registradas.....	14
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD	14
3.2.1. Métodos de prueba de posesión de la clave privada.	14
3.2.2. Autenticación de la identidad de una organización.	14

3.2.3. Autenticación de la identidad de un individuo.	14
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE.	14
3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.	15
3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.	15
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE	15
4. EL CICLO DE VIDA DE LOS CERTIFICADOS.	16
4.1. SOLICITUD DE CERTIFICADOS	16
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.....	16
4.3. EMISIÓN DE CERTIFICADOS	16
4.4. ACEPTACIÓN DE CERTIFICADOS	16
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.....	16
4.6. RENOVACIÓN DE CERTIFICADOS.....	17
4.7. RENOVACIÓN DE CLAVES	17
4.8. MODIFICACIÓN DE CERTIFICADOS.	17
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	17
4.9.1. Circunstancias para la revocación.....	17
4.9.2. Entidad que puede solicitar la revocación	17
4.9.3. Procedimiento de solicitud de revocación	17
4.9.4. Periodo de gracia de la solicitud de revocación	17
4.9.5. Circunstancias para la suspensión.....	17
4.9.6. Entidad que puede solicitar la suspensión	17
4.9.7. Procedimiento para la solicitud de suspensión	17
4.9.8. Límites del período de suspensión	17
4.9.9. Frecuencia de emisión de CRLs	17
4.9.10. Requisitos de comprobación de CRLs	17
4.9.11. Otras formas de divulgación de información de revocación disponibles	17
4.9.12. Requisitos especiales de renovación de claves comprometidas	17
4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....	18
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN.	18
4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES.	18
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES	19

5.1. CONTROLES DE SEGURIDAD FÍSICA	19
5.1.1. Ubicación y construcción	19
5.1.2. Acceso físico.....	19
5.1.3. Alimentación eléctrica y aire acondicionado.....	19
5.1.4. Exposición al agua.....	19
5.1.5. Protección y prevención de incendios	19
5.1.6. Sistema de almacenamiento	19
5.1.7. Eliminación de residuos.....	19
5.1.8. Backup remoto.....	19
5.2. CONTROLES DE PROCEDIMIENTOS.....	19
5.2.1. Papeles de confianza	19
5.2.2. Número de personas requeridas por tarea.....	19
5.2.3. Identificación y autenticación para cada papel.....	19
5.3. CONTROLES DE SEGURIDAD DE PERSONAL.....	19
5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación	19
5.3.2. Procedimientos de comprobación de antecedentes	20
5.3.3. Requerimientos de formación.....	20
5.3.4. Requerimientos y frecuencia de actualización de la formación	20
5.3.5. Frecuencia y secuencia de rotación de tareas	20
5.3.6. Sanciones por acciones no autorizadas.....	20
5.3.7. Requerimientos de contratación de personal	20
5.3.8. Documentación proporcionada al personal	20
5.3.9. Controles periódicos de cumplimiento.....	20
5.3.10. Finalización de los contratos	20
5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....	20
5.4.1. Tipos de eventos registrados	20
5.4.2. Frecuencia de procesado de logs	20
5.4.3. Periodo de retención para los logs de auditoría	20
5.4.4. Protección de los logs de auditoría	20
5.4.5. Procedimientos de backup de los logs de auditoría.....	20
5.4.6. Sistema de recogida de información de auditoría (interno vs externo)	20
5.4.7. Notificación al sujeto causa del evento	21
5.4.8. Análisis de vulnerabilidades	21
5.5. ARCHIVO DE INFORMACIONES Y REGISTROS	21
5.5.1. Tipo de informaciones y eventos registrados	21
5.5.2. Periodo de retención para el archivo.....	21
5.5.3. Protección del archivo.	21
5.5.4. Procedimientos de backup del archivo.....	21
5.5.5. Requerimientos para el sellado de tiempo de los registros.....	21
5.5.6. Sistema de recogida de información de auditoría (interno vs externo).....	21
5.5.7. Procedimientos para obtener y verificar información archivada.....	21
5.6. CAMBIO DE CLAVE.....	21
5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE	21
5.7.1. Alteración de los recursos hardware, software y/o datos.....	21
5.7.2. La clave pública de una entidad se revoca	21
5.7.3. La clave de una entidad se compromete.....	22
5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre	22

5.8. CESE DE UNA CA.....	22
6. CONTROLES DE SEGURIDAD TÉCNICA.....	23
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	23
6.1.1. Generación del par de claves	23
6.1.2. Entrega de la clave privada a la entidad	23
6.1.3. Entrega de la clave pública al emisor del certificado	23
6.1.4. Entrega de la clave pública de la CA a los usuarios	23
6.1.5. Tamaño de las claves.....	23
6.1.6. Parámetros de generación de la clave pública	23
6.1.7. Comprobación de la calidad de los parámetros	23
6.1.8. Hardware/software de generación de claves	24
6.1.9. Fines del uso de la clave	24
6.2. PROTECCIÓN DE LA CLAVE PRIVADA	24
6.2.1. Estándares para los módulos criptográficos.....	24
6.2.2. Control multipersona de la clave privada	24
6.2.3. Custodia de la clave privada.....	24
6.2.4. Copia de seguridad de la clave privada	24
6.2.5. Archivo de la clave privada.....	25
6.2.6. Introducción de la clave privada en el módulo criptográfico.....	25
6.2.7. Método de activación de la clave privada.....	25
6.2.8. Método de desactivación de la clave privada.....	25
6.2.9. Método de destrucción de la clave privada	25
6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....	25
6.3.1. Archivo de la clave pública	25
6.3.2. Periodo de uso para las claves públicas y privadas.....	25
6.4. DATOS DE ACTIVACIÓN	25
6.4.1. Generación y activación de los datos de activación.....	25
6.4.2. Protección de los datos de activación	25
6.4.3. Otros aspectos de los datos de activación	26
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.....	26
6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....	26
6.7. CONTROLES DE SEGURIDAD DE LA RED.....	26
6.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS	26
7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS	27
7.1. PERFIL DE CERTIFICADO	27
7.1.1. Número de versión	27
7.1.2. Extensiones del certificado	27

QCP PUBLIC + SSCD (0.4.0.1456.1.1)	28
7.1.3. Identificadores de objeto (OID) de los algoritmos	30
7.1.4. Formatos de nombres.....	30
7.1.5. Restricciones de los nombres	30
7.1.6. Identificador de objeto (OID) de la Política de Certificación	30
7.1.7. Uso de la extensión “Policy Constraints”	30
7.1.8. Sintaxis y semántica de los cualificadores de política.....	30
7.1.9. Tratamiento semántico para la extensión “Certificate Policy”	30
7.1.10. Tipo de tiempo utilizado en el ciclo de vida de los certificados	30
7.2. PERFIL DE CRL	31
7.2.1. Número de versión	31
7.2.2. CRL y extensiones.....	31
7.3 LISTAS DE CERTIFICADOS REVOCADOS	31
7.3.1 Limite Temporal de los certificados en las CRLs	31
7.4.- PERFIL DE OCSP	31
8. AUDITORÍA DE CONFORMIDAD	32
8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD	32
8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR	32
8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA	32
8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD	32
8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.....	32
8.6. COMUNICACIÓN DE RESULTADOS.....	32
9. REQUISITOS COMERCIALES Y LEGALES	33
9.1. TARIFAS	33
9.1.1. Tarifas de emisión de certificado o renovación	33
9.1.2. Tarifas de acceso a los certificados	33
9.1.3. Tarifas de acceso a la información de estado o revocación	33
9.1.4. Tarifas de otros servicios como información de políticas	33
9.1.5. Política de reintegros	33
9.2. CAPACIDAD FINANCIERA	33
9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACEDICOMMX.	33
9.2.2. Relaciones fiduciarias	33
9.2.3. Procesos administrativos	33
9.3. POLÍTICA DE CONFIDENCIALIDAD	33
9.3.1. Información confidencial.	33
9.3.2. Información no confidencial	33

9.3.3. Divulgación de información de revocación /suspensión de certificados	33
9.4. PROTECCIÓN DE DATOS PERSONALES.....	34
9.4.1. Plan de Protección de Datos Personales.....	34
9.4.2. Información considerada privada.....	34
9.4.3. Información no considerada privada.....	34
9.4.4. Responsabilidades.....	34
9.4.5. Prestación del consentimiento en el uso de los datos personales.....	34
9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales.....	34
9.4.7. Otros supuestos de divulgación de la información.....	34
9.5. DERECHOS DE PROPIEDAD INTELECTUAL	34
9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL	34
9.6.1. Obligaciones de la Entidad de Certificación.....	34
9.6.2. Obligaciones de la Autoridad de Registro.....	34
9.6.3. Obligaciones de los suscriptores.....	34
9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACEDICOMMX34	
9.6.5. Obligaciones del repositorio.....	34
9.7. RENUNCIAS DE GARANTÍAS.....	35
9.8. LIMITACIONES DE RESPONSABILIDAD.....	35
9.8.1. Garantías y limitaciones de garantías.....	35
9.8.2. Deslinde de responsabilidades.....	35
9.8.3. Limitaciones de pérdidas.....	35
9.9. PLAZO Y FINALIZACIÓN.....	35
9.9.1. Plazo.....	35
9.9.2. Finalización.....	35
9.9.3. Supervivencia.....	35
9.10. NOTIFICACIONES.....	35
9.11. MODIFICACIONES.....	35
9.11.1. Procedimientos de especificación de cambios.....	35
9.11.2. Procedimientos de publicación y notificación.....	35
9.11.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación.....	35
9.12. RESOLUCIÓN DE CONFLICTOS.....	35
9.12.1. Resolución extrajudicial de conflictos.....	36
9.12.2. Jurisdicción competente.....	36
9.13. LEGISLACIÓN APLICABLE	36
9.14. CONFORMIDAD CON LA LEY APLICABLE.....	36
9.15. CLÁUSULAS DIVERSAS.....	36

1. INTRODUCCIÓN

1.1. PRESENTACIÓN

EDICOMUNICACIONES, S.A. de C.V. (en adelante EDICOM) se constituye en Prestador de Servicios de Certificación o Autoridad de Certificación con el objetivo de implementar los Servicios de Seguridad Administrados para la Infraestructura de Llave Pública (PKI), a partir de una revisión metodológica acorde a las mejores prácticas internacionales en materia de seguridad de la información y la aplicación de las leyes y normativas existentes en México.

El presente documento es la Política de Certificación asociada a los **certificados de Firma Electrónica Fiable con limitación de uso sobre dispositivo seguro (SSCD)**, que contiene las reglas a las que se sujeta el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Autoridad de Certificación EDICOM México(ACEDICOMMX) y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la *Declaración de Prácticas de Certificación (CPS)* de la ACEDICOMMX.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados de firma fiable sobre dispositivo seguro (SSCD) para ser utilizados dentro del ámbito general de las aplicaciones de firma electrónica.

Este tipo de certificados se expiden con un periodo de vigencia de 2 años.

Mediante los certificados en dispositivo seguro asociados a esta Política de Certificación se generarán firmas electrónicas avanzadas o fiables según el artículo 97 del Código de Comercio.

La presente Declaración de Prácticas de Certificación está redactada siguiendo las especificaciones del RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"* propuesto por *Network Working Group* y completada con aspectos exigidos en la ETSI TS 101 456 V1.2.1 *"Policy Requirements for certification authorities issuing qualified certificates"*, al igual que la Declaración de Prácticas de Certificación, para facilitar la lectura o comparación con documentos homólogos.

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

REFORMAS AL CODIGO DE COMERCIO

- Reformas al Código de Comercio en materia de firma electrónica publicadas el 29 de agosto del 2003 en el D.O.F.
- Reformas al Código de Comercio en materia de firma electrónica publicadas el 29 de mayo del 2000 en el D.O.F.

NORMAS OFICIALES

- NORMA Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos publicada el 4 de junio del 2002 en el D.O.F.

REGLAMENTOS Y REGLAS

- Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación (Publicado el 19 de julio del 2004 en el D.O.F.)
- Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación (Publicadas el 10 de agosto del 2004 en el D.O.F.)
- ACUERDO que modifica las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación (Publicado el 5 de marzo del 2007 en el D.O.F.)

Esta Política de Certificación asume que el lector conoce los conceptos básicos de Infraestructura de Clave Pública (PKI), certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2. IDENTIFICACIÓN

Nombre del documento	Política de Certificación de Certificados de Firma Electrónica Fiable con limitación de uso sobre dispositivo seguro (SSCD)
Calificador de la política:	Certificado cualificado expedido por la ACEDICOMMX
Versión del documento	1.1
Estado del documento	Vigente
OID (Object Identifier)	1.3.6.1.4.1.30051.2.2.2.1.1
Fecha de emisión	03 de Octubre de 2008
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX. Versión 1.1 OID: 1.3.6.1.4.1.30051.2.2.1.1 Disponible en : http://acedicom.edicomgroup.com/mx
Localización	http://acedicom.edicomgroup.com/mx

1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN

1.3.1. Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es “ACEDICOMMX”.

1.3.2. Autoridades de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

1.3.3. Usuarios Finales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos Permitidos

Los certificados emitidos por la ACEDICOMMX bajo esta Política de Certificación son certificados cualificados de firma electrónica fiable y pueden utilizarse en aplicaciones que requieran el uso de esta tecnología con la limitación de uso por razón de ámbito que se establezca en la extensión **1.3.6.1.4.1.30051.3.2** de forma textual, publicándose las limitaciones posibles en el apartado “Limitaciones de uso” de ésta política de certificación en la web de la ACEDICOMMX <http://acedicom.edicomgroup.com/mx>, y que son las siguientes:

- “Conservación de mensajes de datos NOM-151”
- “Control de accesos” , autenticación de usuarios

En caso de no establecerse ninguna limitación de uso, el certificado podrá ser utilizado para firma de documentos con propósito general. En todo caso es el Solicitante del certificado el responsable del cumplimiento del ámbito de uso permitido con las limitaciones establecidas.

Este certificado (**certificado cualificado** según ETSI y la RFC3739) permite la generación de firmas electrónicas avanzadas o fiables según el artículo 97 del Código de Comercio.

El uso de estos certificados proporciona las siguientes garantías:

- **No repudio de origen**

Asegura que el documento proviene del suscriptor de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del Certificado de Firma. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando el servicio de validación de ACEDICOMMX. De esta forma garantiza que el documento proviene de un determinado suscriptor.

Dado que este certificado se emite sobre un dispositivo seguro de creación de firma y que las claves de firma permanecen desde el momento de su creación bajo el control del suscriptor titular, se garantiza el compromiso del mismo con la firma realizada (garantía de “no repudio”).

- **Integridad**

Con el empleo del Certificado de Firma, se permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de su resumen.

- El uso de este certificado, no significa que se esté dando el acuerdo sobre el contenido del documento firmado.

1.4.2. Usos prohibidos

Los certificados se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política de Certificación, y con arreglo a la normativa vigente.

1.4.3. Fiabilidad de la firma electrónica a lo largo del tiempo

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas deberá existir un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

La generación de una firma longeva debe incluir los siguientes elementos:

Sello de tiempo: Se ha de incluir en la firma un sello de tiempo emitido por una Tercera Parte de Confianza, TSA (Autoridad de Sellado de Tiempo). El sello de tiempo asegura que tanto los datos originales del documento como la información del estado de los certificados, se generaron antes de una determinada fecha. El formato del sello de tiempo debe seguir el estándar definido en la RFC3161.

Información de revocación: La firma ha de incluir un elemento que asegura que el certificado de firma es válido. Este elemento será generado una Tercera Parte de Confianza, en este caso por la ACEDICOMMX.

Es necesario que con posterioridad las firmas puedan renovarse (refirmado) y actualizar los elementos de confianza (sellos de tiempo) para dotar a las firmas electrónicas de validez a lo largo del tiempo, logrando garantizar su fiabilidad.

1.5. POLÍTICA DE ADMINISTRACIÓN

1.5.1. Especificación de la Organización Administradora

Nombre	Dirección Técnica de EDICOM
Dirección de email	ACEDICOMMX@edicomgroup.com
Dirección	Río Lerma No. 302 Piso 5 Oficina 503 Colonia Cuauhtémoc C.P. 06500 Delegación Cuauhtémoc en México, D.F.
Número de teléfono	[55] 52-12-15-66

1.5.2. Persona de Contacto

Nombre	Departamento de sistemas de EDICOM
Dirección de email	ACEDICOMMX@edicomgroup.com
Dirección	Río Lerma No. 302 Piso 5 Oficina 503 Colonia Cuauhtémoc C.P. 06500 Delegación Cuauhtémoc en México, D.F.
Número de teléfono	[55] 52-12-15-66

1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas

La Dirección Técnica de EDICOM es el Órgano competente para determinar la adecuación de esta Política de Certificación a la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

No estipulado

1.6.2. Acrónimos

No estipulado

2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1. REPOSITORIO DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

2.2. PUBLICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

2.3. FRECUENCIA DE ACTUALIZACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

Las especificaciones contenidas en este apartado complementan estipulaciones previstas la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX en caso de ser necesario.

3.1. REGISTRO DE NOMBRES

3.1.1. Tipos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.1.2. Significado de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.1.3. Interpretación de formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.1.4. Unicidad de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.1.5. Resolución de conflictos relativos a nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.1.6. Reconocimiento, autenticación y función de las marcas registradas.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1. Métodos de prueba de posesión de la clave privada.

Los pares de claves asociados a los certificados de esta política se generan mediante un proceso controlado en todo momento por el solicitante utilizando un dispositivo seguro de creación de firma SSCD certificado CWA 14169 (CC EAL4+) que obra bajo su poder, garantizando que en todo momento las claves privadas están bajo su control mediante mecanismos de protección basados en la posesión de la tarjeta y número PIN. La generación de claves sólo puede ser realizada mediante la aplicación preparada para tal fin por EDICOM que contempla la autenticación segura del solicitante frente a esta aplicación y mediante la cual se establece un canal seguro con el dispositivo SSCD. Las claves privadas se generan en el dispositivo y no pueden ser exportadas en ningún formato y sólo se pueden utilizar conociendo el correspondiente número PIN.

3.2.2. Autenticación de la identidad de una organización.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.2.3. Autenticación de la identidad de un individuo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE.

3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4. EL CICLO DE VIDA DE LOS CERTIFICADOS.

Las especificaciones contenidas en este apartado complementan estipulaciones previstas en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX en caso de ser necesario.

4.1. SOLICITUD DE CERTIFICADOS

La entidad o persona que desee le sea emitido un certificado de acuerdo con esta política de certificación deberá solicitarlo a través del documento “CONTRATO DE PRESTACION DE SERVICIOS DE CERTIFICACION DIGITAL” que puede obtener en la página web de la ACEDICOMMX <http://acedicom.edicomgroup.com/mx> en el Área “Gestion de Certificados”.

En el momento de formalizar su solicitud, el solicitante deberá acreditar su identidad de forma presencial o remota ante cualquier Punto de registro autorizado, tal como se describe en la CPS (Declaración de Prácticas de Certificación) punto 3.2.3, presentar el “CONTRATO DE PRESTACION DE SERVICIOS DE CERTIFICACION DIGITAL” debidamente firmado y, en su caso, la documentación que corresponda con arreglo al tipo de entidad y representación tal como se indica en el CPS punto 3.2.2.

A estos efectos se podrá prescindir de la presencia física si la firma contenida en el Contrato ha sido legitimada notarialmente.

El encargado de recibir dicha documentación en la Entidad de Registro, comprobará la identidad del solicitante y verificará los documentos acreditativos de su representación así como su inscripción en el correspondiente registro público, si resultara exigible.

Hechas todas estas comprobaciones se valida la solicitud en el sistema informático enviándola electrónicamente y de forma segura a la ACEDICOMMX. En el caso de denegación de la solicitud de certificación por parte del Operador de la Autoridad de Registro, el solicitante recibirá información de los motivos del rechazo de la misma.

Obtenido/s el/los certificado/s el solicitante recibirá una notificación por Email de los detalles y atributos del/os mismo/s.

El listado de Puntos de registro autorizados se encuentra en la página web <http://acedicom.edicomgroup.com/mx> en el Área “Puntos de Registro”.

4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.3. EMISIÓN DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.4. ACEPTACIÓN DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.

Los certificados ACEDICOMMX bajo esta política son certificados reconocidos de firma para el ámbito general, destinados a personas físicas o a entidades jurídicas (colectivamente llamados suscriptores).

Los Terceros Aceptantes sólo pueden depositar su confianza en los certificados para aquello que establece este documento y de acuerdo con lo establecido en el campo ‘Key Usage’ del certificado.

4.6. RENOVACIÓN DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.7. RENOVACIÓN DE CLAVES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.8. MODIFICACIÓN DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.

4.9.1. Circunstancias para la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.2. Entidad que puede solicitar la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.3. Procedimiento de solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.4. Periodo de gracia de la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.5. Circunstancias para la suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.6. Entidad que puede solicitar la suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.7. Procedimiento para la solicitud de suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.8. Límites del período de suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.9. Frecuencia de emisión de CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.10. Requisitos de comprobación de CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.11. Otras formas de divulgación de información de revocación disponibles

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.9.12. Requisitos especiales de renovación de claves comprometidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES.

La ACEDICOM no realiza en este caso el depósito de claves de firma, si no que éstas se generan en el dispositivo que está en poder exclusivo del propio suscriptor (SSCD) certificado CC EAL 4+ bajo Protection Profile de Secure Signature Creation Device (SSCD) definido según CWA 14169. Los únicos que tienen acceso a las claves de firma son los propietarios de las mismas mediante la posesión del mismo y utilizando para ello las claves de activación que obran exclusivamente en su poder.

Las claves privadas no son exportables en ningún caso.

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

5.1. CONTROLES DE SEGURIDAD FÍSICA

5.1.1. Ubicación y construcción

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.1.2. Acceso físico

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.1.3. Alimentación eléctrica y aire acondicionado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.1.4. Exposición al agua

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.1.5. Protección y prevención de incendios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.1.6. Sistema de almacenamiento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.1.7. Eliminación de residuos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.1.8. Backup remoto

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.2. CONTROLES DE PROCEDIMIENTOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.2.1. Papeles de confianza

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.2.2. Número de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.2.3. Identificación y autenticación para cada papel

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3. CONTROLES DE SEGURIDAD DE PERSONAL

5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.2. Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.3. Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.5. Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.6. Sanciones por acciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.7. Requerimientos de contratación de personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.8. Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.9. Controles periódicos de cumplimiento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.3.10. Finalización de los contratos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

5.4.1. Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4.2. Frecuencia de procesado de logs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4.3. Periodo de retención para los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4.4. Protección de los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4.5. Procedimientos de backup de los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4.6. Sistema de recogida de información de auditoría (interno vs externo)

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4.7. Notificación al sujeto causa del evento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.4.8. Análisis de vulnerabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.5. ARCHIVO DE INFORMACIONES Y REGISTROS

5.5.1. Tipo de informaciones y eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.5.2. Periodo de retención para el archivo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.5.3. Protección del archivo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.5.4. Procedimientos de backup del archivo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.5.5. Requerimientos para el sellado de tiempo de los registros.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.5.6. Sistema de recogida de información de auditoría (interno vs externo).

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.5.7. Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.6. CAMBIO DE CLAVE

No estipulado.

5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.7.1. Alteración de los recursos hardware, software y/o datos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.7.2. La clave pública de una entidad se revoca

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.7.3. La clave de una entidad se compromete

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

5.8. CESE DE UNA CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.1 de la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6.1.1. Generación del par de claves

Los pares de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en el dispositivo que está en poder exclusivo del propio suscriptor (SSCD) certificado CC EAL 4+ bajo Protection Profile de Secure Signature Creation Device (SSCD). Los únicos que tienen acceso a las claves de firma son los propietarios de las mismas mediante la posesión del mismo y utilizando para ello las claves de activación que obran exclusivamente en su poder.

Las claves privadas no son exportables en ningún caso.

6.1.2. Entrega de la clave privada a la entidad

La clave privada se genera mediante un proceso iniciado por el propio titular en el dispositivo criptográfico que obra en su poder y no es posible la extracción de la misma. No existe por tanto ninguna transferencia de clave privada.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada en el interior del dispositivo criptográfico seguro en poder del suscriptor y es enviada a la PKI ACEDICOMMX formando parte de una solicitud en formato PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

6.1.4. Entrega de la clave pública de la CA a los usuarios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6.1.5. Tamaño de las claves

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es de 1024 bits mínimo.

6.1.6. Parámetros de generación de la clave pública

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI SR 002 176 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature".

Signature algorithm Signature algorithm parameters

Rsa MinModLen=1020

Key generation algorithm

rsagen1

Padding method Cryptographic

emsa-pkcs1-v1_5

Hash function

sha1

6.1.7. Comprobación de la calidad de los parámetros

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI SR 002 176 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature".

6.1.8. Hardware/software de generación de claves

El par de claves se generan en el dispositivo que está en poder exclusivo del propio suscriptor (SSCD) certificado CC EAL 4+ bajo Protection Profile de Secure Signature Creation Device (SSCD). Los únicos que tienen acceso a las claves de firma son los propietarios de las mismas mediante la posesión del mismo y utilizando para ello las claves de activación que obran exclusivamente en su poder. Las claves privadas no son exportables en ningún caso.

6.1.9. Fines del uso de la clave

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento *1.3 Comunidad de usuarios y ámbito de aplicación*.

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 de este documento "*Perfiles de certificado y listas de certificados revocados*".

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por ACEDICOMMX.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.2 de la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6.2.1. Estándares para los módulos criptográficos

El dispositivo criptográfico seguro empleado en la emisión de los certificados adscritos a esta Política de Certificación dispone de certificación CC EAL4+ y CWA 14169.

6.2.2. Control multipersona de la clave privada

Las claves privadas para los certificados de firma emitidos bajo el ámbito de la presente Política de Certificación se encuentran depositadas en el dispositivo seguro de creación de firma que obra en poder del suscriptor y protegido por mecanismos basados en número PIN. Las claves privadas no son exportables en ningún caso.

6.2.3. Custodia de la clave privada

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran contenida en el dispositivo criptográfico seguro que obra en poder del suscriptor, por lo tanto la ACEDICOMMX no realiza ningún tipo de custodia sobre las claves privadas asociadas a esta política.

Las Claves Privadas del suscriptor se encuentran almacenadas en el procesador de las tarjeta criptográfica del dispositivo que obra en su poder. Para acceder a dicha clave el suscriptor debe introducir un número PIN que sólo él debe conocer.

6.2.4. Copia de seguridad de la clave privada

Por motivos de seguridad no es posible hacer copias de seguridad de las claves privadas de firma de los usuarios.

6.2.5. Archivo de la clave privada.

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran contenidas en cada uno de los dispositivo criptográficos que obran en el poder de los respectivos suscriptores.

6.2.6. Introducción de la clave privada en el módulo criptográfico.

La generación de las claves vinculadas al certificado de firma se realiza dentro del dispositivo criptográfico y nunca lo abandonan.

6.2.7. Método de activación de la clave privada.

Para el acceso a las claves y al certificado de firma el suscriptor deberá emplear su tarjeta criptográfica y una clave personal de acceso (PIN) generada en el momento de generar su certificado y que sólo él debe conocer.

6.2.8. Método de desactivación de la clave privada

La desactivación de la clave privada del suscriptor se consigue mediante la extracción de la tarjeta criptográfica que la contiene del lector PC/SC.

6.2.9. Método de destrucción de la clave privada

En términos generales la destrucción siempre debe ser precedida por una revocación del certificado asociado a la clave, si éste estuviese todavía vigente.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.

6.3.1. Archivo de la clave pública

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6.3.2. Periodo de uso para las claves públicas y privadas

Los certificados emitidos al amparo de la presente política tienen una validez de dos (2) años. El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de dos (2) años.

La caducidad producirá automáticamente la invalidación de los Certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación y activación de los datos de activación

Los datos de activación de la clave privada consisten en la posesión de la tarjeta criptográfica y un número PIN de acceso al hardware criptográfico.

Es el propio suscriptor el que genera el par de claves en la tarjeta. Cuando el suscriptor solicita la generación del par de claves introduce un número PIN que sólo él conoce y que servirá como clave de activación para generar cualquier firma posterior. Es responsabilidad y obligación del suscriptor el control de dicho PIN.

6.4.2. Protección de los datos de activación

El suscriptor del certificado es el responsable de la protección de los datos de activación de su clave privada.

6.4.3. Otros aspectos de los datos de activación

No estipulado.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6.7. CONTROLES DE SEGURIDAD DE LA RED

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

6.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

7.1. PERFIL DE CERTIFICADO

7.1.1. Número de versión

Los certificados de identidad pública emitidos por la AC Subordinada utilizan el estándar X.509 versión 3 (X.509 v3)

7.1.2. Extensiones del certificado

Las extensiones utilizadas en los certificados son:

- *KeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *Subject Directory Attributes*. Calificada como no crítica.
- *CRLDistributionPoints*. Calificada como no crítica.
- *Authority Information Access*. Calificada como no crítica.
- *Qcstatements*. Calificada como no crítica.
- *LimitaciónDeUso* (1.3.6.1.4.1.30051.3.2). Calificada como no crítica

El perfil de los certificados emitidos bajo esta política son:

Campo	Contenido	I	C	T
Versión	v3	S		F
Serial Number	Asignado automáticamente por la AC	S		F
Signature Algorithm	SHA1withRSAEncryption	S		F
Issuer Distinguished Name(*)		S		F
CommonName (CN)	ACEDICOMMX	S		D
Organizational Unit (OU)	PKI	O		D
Organization (O)	EDICOMUNICACIONES MEXICO S.A. de .C.V.	S		D
Country (C)	MX	S		D
Location (L)	Cuauhtemoc			
Street (STREET)	Río Lerma nº 302 Piso 5 Oficina 503			
State (ST)	Distrito Federal			
Email (E)	ACEDICOMMX@edicomgroup.com			
PostalCode	06500			
Número de serie	EME-000602-QR9			
Validez	2 años	S		F
Subject Public Key Info	Tipo de clave: RSA Longitud de la clave: 2048 bits	S		F
Subject		S		D
CommonName (CN)	Apellidos, Nombre	S		D
SerialNumber (SN)	Identificación Fiscal	S		D
GivenName (GN)	Nombre	S		D
Surname (S)	Apellidos	S		D
DN Qualifier	Código de identificación unívoco asignado por el emisor del certificado.	S		D
Organization (O)	Organización a la que pertenece	S		D
Country (C)	País de la organización (no tiene por qué coincidir con la nacionalidad del sujeto)	S		D
Identificación fiscal de la organización representada 1.3.6.1.4.1.30051.3.1.1	OID propio.	C		D
Subject Alternative Names				
E-Mail (RFC 822)	Dirección de E-Mail del sujeto	O		D

SubjectKeyIdentifier	Identificador de la clave pública del certificado	S		D
AuthorityKeyIdentifier	Identificador de la clave pública asociada a la clave privada de la CA usada para firmar el presente certificado	S		F
BasicConstraints		S	X	F
CA	Falso	S	X	F
pathLength	No aplicable (0)			F
KeyUsage	digitalSignature	S	X	F
Certificate Policies		S		F
policyIdentifier	1.3.6.1.4.1.30051.2.2.2.1.1	S		F
CPSURI	http://acedicom.edicomgroup.com/mx	S		F
policyIdentifier	1.3.6.1.4.1.30051.2.2.2.1.1	S		F
userNotice	Certificate Policy for Qualified Certificates for signing with usage limitation	S		F
policyIdentifier	QCP Public + SSCD (0.4.0.1456.1.1)	S		F
LimitaciónDeUso 1.3.6.1.4.1.30051.3.2				
ExtendedKeyUsage	- no aplica -	C		F
CRLDistributionPoints		S		F
distributionPoint	http://acedicom.edicomgroup.com/mx/acedicommx.crl	S		F
Authority Information Access		S		F
accessMethod	Calssuers	S		F
AccessLocation	http://acedicom.edicomgroup.com/certs/acedicommx.cer	S		F
accessMethod	OCSP	S		F
AccessLocation	http://ocsp.acedicom.edicomgroup.com/acedicommx	S		F
QC Statements (id-pe-qcStatements)		S		F
QCSyntax-v2	- Presente -	S		F
QCRetentionPeriod	13	S		F
ETSI QcCompliance	- Presente -	S		F
ETSI QcSSCD	- Presente -	S		F

Leyenda de la tabla:

I = Incluida. Posibles valores: S=Siempre, O=Opcionalmente, C=Condicionalmente

C = Crítica. Si se marca la casilla, indica que es crítica.

T = Tipo. Posibles valores: D = Dinámica, F = Fijada. Fijada quiere decir que el valor es el mismo para todos los certificados de este tipo.

(*) En el campo Issuer falta consignar los datos de acreditación ante la Secretaría que se tendrán una vez que la ACEDICOMMX obtenga la acreditación.

Los certificados emitidos bajo esta política se emiten en calidad de certificados cualificados para generación de **firma fiable** y, por tanto este perfil contiene los campos que establece la normativa legalmente aplicable en esta materia:

Requisitos Legales y deseables	Modo de cumplimiento
La indicación que se expiden como certificados reconocidos	Inclusión de la extensión Qualified Certificate Statements que incorpora las siguientes declaraciones: 1.- id-etsi-qcs-QcCompliance – Indica que el certificado se emite como cualificado. 2.- id-etsi-qcs-QcSSCD – Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo seguro de creación de firma.
La identificación del prestador de servicios	A través de la información que se recoge

<p>de certificación que expide el certificado y el país en el que está establecido</p>	<p>en el campo Issuer del certificado tal y como contempla la rfc 3739 En el certificado se recoge claramente el país en el que se establece el PSC en el atributo Country del DN del campo Issuer En la presente política referenciadas en el certificado, se recoge el nombre o razón social, domicilio, dirección electrónica y número de identificación fiscal de la Institución que actúa como PSC de la ACEDICOMMX: EDICOM.</p>
<p>La identificación del firmante (el suscriptor del certificado), por su nombre y apellidos e Identificación Fiscal o equivalente, o a través de un seudónimo que conste de manera inequívoca.</p>	<p>A través de la información que se recoge en el campo Subject del certificado tal y como contempla la rfc 3739: Nombre, Apellidos e Identificación Fiscal. También organización que representa e Identificación fiscal de la organización Se contempla la inclusión de la extensión Subject Alternative Names para indicar el email de contacto</p>
<p>La inclusión de algún atributo del firmante (el suscriptor), relevante para el uso establecido para el certificado en la Política.</p>	<p>Se incluye dentro del Subject un OID específico (1.3.6.1.4.1.30051.3.1.1) para indicar la Identificación Fiscal de la organización representada</p>
<p>Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.</p>	<p>La clave pública del suscriptor se encuentra en el certificado tal y como contempla la RFC 3280. (Subject Public Key Info)</p>
<p>El comienzo y el final del periodo de validez del certificado.</p>	<p>El periodo de validez de las claves y el certificado asociado se encuentra recogido en el campo del certificado contemplado en la ITU-T Recommendation X.509 y en RFC 3280</p>
<p>El código identificativo único del certificado.</p>	<p>La pareja formada por el Número de serie del certificado y el Issuer tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 3280</p>
<p>La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.</p>	<p>La firma digital del emisor del certificado de acuerdo con la ITU-T Recommendation X.509 y la RFC 3280</p>
<p>Los límites de uso del certificado, si se prevén.</p>	<p>Estos límites están reflejados en la Política de Certificación asociada a este certificados y en la extensión KeyUsage tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 3280. En este caso <i>digitalSignature</i> También se incluye el atributo <i>LímiteDeUso</i> (1.3.6.1.4.1.30051.3.2)</p>

Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.	No estipulado
Necesidad de un servicio de comprobación del estado de los certificados.	La extensión AIA (Authority Information Access) contiene la URL del servicio de validación de certificados
Periodo mínimo de retención de la información relevante	En QCStatements se ha contemplado un periodo de 13 años adicionales a los 2 de vigencia del certificado, en total 15 años.
Los términos y condiciones de uso de los certificados deben estar accesibles a las terceras partes que hacen uso del certificado.	En la extensión CertificatePolicies se indica la URL en la que están accesibles la DPC y las Políticas de Certificación asociadas al certificado

7.1.3. Identificadores de objeto (OID) de los algoritmos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7.1.4. Formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7.1.5. Restricciones de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7.1.6. Identificador de objeto (OID) de la Política de Certificación

El identificador de objeto definido por ACEDICOMMX para identificar la presente política es el siguiente: 1.3.6.1.4.1.30051.2.2.2.1.1

7.1.7. Uso de la extensión “Policy Constraints”

No se hace uso de la extensión “*Policy Constraints*” en los certificados emitidos bajo la presente Política de Certificación.

7.1.8. Sintaxis y semántica de los cualificadores de política

No estipulado

7.1.9. Tratamiento semántico para la extensión “Certificate Policy”

La extensión “*Certificate Policy*” identifica la política que define las practicas que ACEDICOMMX asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un cualificador de la política.

Certificate Policies		S		F
policyIdentifier	1.3.6.1.4.1.30051.2.2.2.1.1	S		F
CPSuri	http://acedicom.edicomgroup.com/mx	S		F
policyIdentifier	1.3.6.1.4.1.30051.2.2.2.1.1	S		F
userNotice	Certificate Policy for Qualified Certificates for signing with usage limitation	S		F
policyIdentifier	QCP Public + SSCD (0.4.0.1456.1.1)	S		F

7.1.10. Tipo de tiempo utilizado en el ciclo de vida de los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7.2. PERFIL DE CRL

7.2.1. Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7.2.2. CRL y extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7.3 LISTAS DE CERTIFICADOS REVOCADOS

7.3.1 Limite Temporal de los certificados en las CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

7.4.- PERFIL DE OCSP

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

8. AUDITORÍA DE CONFORMIDAD

8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

8.6. COMUNICACIÓN DE RESULTADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9. REQUISITOS COMERCIALES Y LEGALES

9.1. TARIFAS

9.1.1. Tarifas de emisión de certificado o renovación

La emisión de certificados digitales bajo la presente política de certificación está sometida a unas tarifas fijadas por EDICOM. Los precios públicos actualizados se recogen en la web de la ACEDICOMMX.

9.1.2. Tarifas de acceso a los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.1.3. Tarifas de acceso a la información de estado o revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.1.4. Tarifas de otros servicios como información de políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.1.5. Política de reintegros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.2. CAPACIDAD FINANCIERA

9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACEDICOMMX.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.2.2. Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.2.3. Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.3. POLÍTICA DE CONFIDENCIALIDAD

9.3.1. Información confidencial.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.3.2. Información no confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.3.3. Divulgación de información de revocación /suspensión de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4. PROTECCIÓN DE DATOS PERSONALES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4.1. Plan de Protección de Datos Personales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4.2. Información considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4.3. Información no considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4.4. Responsabilidades.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4.5. Prestación del consentimiento en el uso de los datos personales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.4.7. Otros supuestos de divulgación de la información.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX..

9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL

9.6.1. Obligaciones de la Entidad de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.6.2. Obligaciones de la Autoridad de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.6.3. Obligaciones de los suscriptores

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACEDICOMMX

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.6.5. Obligaciones del repositorio

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.7. RENUNCIAS DE GARANTÍAS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.8. LIMITACIONES DE RESPONSABILIDAD

9.8.1. Garantías y limitaciones de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.8.2. Deslinde de responsabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.8.3. Limitaciones de pérdidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.9. PLAZO Y FINALIZACIÓN.

9.9.1. Plazo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.9.2. Finalización.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.9.3. Supervivencia.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.10. NOTIFICACIONES.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.11. MODIFICACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.11.1. Procedimientos de especificación de cambios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.11.2. Procedimientos de publicación y notificación.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.11.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.12. RESOLUCIÓN DE CONFLICTOS.

9.12.1. Resolución extrajudicial de conflictos.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.12.2. Jurisdicción competente.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.13. LEGISLACIÓN APLICABLE

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.14. CONFORMIDAD CON LA LEY APLICABLE.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.

9.15. CLÁUSULAS DIVERSAS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOMMX.