Ley de Firma Digital de la República Federal Alemana

Articulo 1: Objetivo y Area de Aplicación. ➦

El propósito de esta ley es crear condiciones generales para firmas digitales bajo las cuales se las pueda considerar seguras y que las falsificaciones de firmas digitales y falsificaciones de información firmada puedan ser verificados sin lugar a duda.

La aplicación de otros procedimientos para firmas digitales está permitida en la medida que las firmas digitales no son requeridas legalmente bajo esta ley.

Articulo 2: Definiciones. ➦

Una firma digital dentro del significado de esta ley es un sello creado con una clave privada de firmas sobre información digital, tal sello permite, mediante el uso de la clave publica asociada rotulada por un certificado de clave de un certificador, o de una Autoridad según el artículo 3, que sean verificados el propietario de la clave de firma y el carácter de no falsificado de la información sean verificados.

Un certificador dentro del significado de esta ley, es una persona física o jurídica la cual da fe a la atribución de claves públicas de firma a personas físicas y mantiene una licencia para ese motivo según articulo 4.

Un certificado, dentro del significado de esta ley es una certificación digital rotulada con una firma digital respecto a la atribución de una clave de firma publica a una persona física (certificado de clave de firma), o una certificación digital especial que se refiere inequívocamnte a un certificado de clave de firma y contiene información adicional

(certificado de atributos).

Un sellado de fecha y hora dentro del significado de esta ley es una certificación digital de un certificado rotulado con una firma digital de que cierta información digital fue presentada en determinado momento.

Articulo 3: La autoridad. ➦

La otorgación de licencias y la emisión de certificados los cuales serán utilizados para firmar certificados y los certificadores así como la supervisión del cumplimiento de esta Ley y de la Ordenanza Legal del Articulo 16, yace bajo la Autoridad según el Articulo 66 de la Ley de Telecomunicaciones.

Articulo 4: Otorgación de licencias para certificantes. ➦

La operación de un certificador requiere de una licencia de la Autoridad, la cual será otorgada a solicitud.

La licencia será denegada si hay bases contundentes para la suposición que el solicitante no es lo suficientemente confiable para operar como certificador, si el solicitante no demuestra poseer el conocimiento necesario para operar como certificador o si se puede suponer que los posteriores requerimientos para la operación como certificador - bajo esta ley y la Ordenanza Legal según Articulo 16- no estarán presentes una vez iniciadas las operaciones.

Un solicitante posee la confiabilidad necesaria si puede garantizar que cumplirá como poseedor de licencia con los requerimiento legales relevantes para operar como certificador. El conocimiento necesario esta presente si aquellas personas trabajando en el certificador tienen el conocimiento, experiencia y calificación necesarios. Los siguientes requerimientos para la operación del certificador están presentes si las medidas para el cumplimiento de los requerimiento de seguridad de esta Ley y la Ordenanza Legal según Articulo 16 están registradas en un plan de seguridad, cuya implementación ha sido examinada y verificada por una instancia reconocida por la Autoridad.

La licencia puede contener cláusulas complementarias en la medida que estas sean necesarias para asegurar que el certificante cumpla con los requerimientos de esta Ley y la Ordenanza Legal según el Articulo 16 una vez comenzadas las operaciones y durante ellas.

La Autoridad emite los certificados para claves de firma que se utilizarán para firmar certificados. Las disposiciones para la emisión de certificados por los certificadores se aplican correspondientemente a la Autoridad, la que debe mantener acceso en todo momento y para todos a los certificados que ha emitido en todo momento y para todos, a través de conexiones de telecomunicaciones accesibles al público. Esto también se aplica para información que respecta a direcciones y números telefónicos de certificadores, el bloqueo de certificados que ella haya emitido, la finalizacón y prohibición del desarrollo de actividades licenciadas.

Se impondrán costos (aranceles y gastos) por los servicios públicos bajo esta Ley y el Decreto a que se refiere el párrafo 16.

Articulo 5: Emisión de certificados de claves de firmas y sellos de fecha y hora. ➦

El certificador deberá identificar fehacientemente a las personas que soliciten certificados. Deberá confirmar la atribución de una clave publica de firma a una persona identificada mediante un certificado de claves de firma y mantendrá acceso a estos, así como a los certificados asociados (párrafo 2), en todo momento y para cualquier persona, a través de conexiones de telecomunicaciones accesibles públicamente de una manera verificable y con el consentimiento del dueño de la clave de firma, salvo pedido explícito de no publicación por parte del suscriptor.

Bajo pedido de un solicitante, el certificador registrará información concerniente al poder de representación de una tercera parte o sus licencias profesionales u otras en el certificado de clave de firma o en un certificado de atributos, en tanto se demuestra fehacientemente el consentimiento de la tercera parte para que tal licenciamiento o poder de representación sean registradas en un certificado.

A pedido de un solicitante, el certificador deberá registrar un seudónimo en el certificado en el lugar del nombre del solicitante.

El certificador deberá tomar medidas para que la información de los certificados no puedan ser alterados o falsificados de manera no visible. Deberá tomar medidas de modo que se garantice la confidencialidad de la clave privada. No es confiable el almacenamiento de claves privadas por parte del certificador.

(Nota del los Traductores: El contenido es cuestionable. "El certificador nunca debe tomar contacto con las claves privadas de los suscriptores." Alemás existen divergencias entre la versione de inglés y la alemana.)

El certificador deberá usar personal confiable para el ejercicio de las actividades de certificación y deberá usar componentes técnicos de acuerdo a lo expresado en el articulo 14 para hacer accesibles las claves y para la generación de certificados. Esto se aplica también a componentes técnicos que hacen posible la verificación de los certificados según párrafo 1, sentencia 2.

Articulo 6: Deber de informar. ➦

El certificador deberá informar al solicitante en lo referente al articulo 5 párrafo 1 concierniente a las medidas necesarias para contribuir a asegurar la firma digital y su verificación confiable. Deberá informar al solicitante respecto a los componentes técnicos que cumplan los requerimientos del Articulo 14 párrafo 1 y 2, como también lo concerniente a la atribución de firmas digitales creadas con una clave privada. Deberá señalar al solicitante que la información con firma digital puede necesitar ser refirmada antes que el valor de seguridad de una firma disponible decrezca con el tiempo.

(Nota de los Traductores: Omite detalles importantes que el suscriptor debe conocer y que constituye su responsabilidad)

Articulo 7: Contenido de los certificados. ➦

Un certificado de clave de firma deberá contener al menos lo siguiente :

El nombre del dueño de la clave de firma, el cual se marca con una notación adicional si existe la posibilidad de confusión, o con un seudónimo inequívoco atribuible al dueño de la clave, el cual deberá ser identificado como tal;

La clave publica de firma atribuida;

El nombre de los algoritmos que pueden usarse con la clave publica del usuario, así como con la clave publica del certificador;

El número de serie del certificado;

El comienzo y el fin de la validez del certificado;

El nombre del certificador; y

Información acerca de la limitación de uso de la clave de firma a determinados tipos y ámbitos de aplicación;

Información concerniente al poder de representación para una tercera parte, o concerniente a licencias profesionales u otras que pueden registrarse en el certificado de clave de firma o en un certificado de atributos.

(Nota de los Traductores: Debería incluir la fecha de emisión del certificado.)

Articulo 8: Bloqueo de certificados. ➦

Un certificador deberá bloquear un certificado a pedido del dueño de la clave de firma o de su representante, si el certificado fue expedido basándose en información falsa según lo expresado en el Articulo 7, si el certificador ha finalizado sus actividades y estas no fueron continuadas por otro certificador, o si la Autoridad ordena un bloqueo según lo expresado en el Articulo 13 párrafo 5 sentencia 2. El bloqueo deberá indicar el momento desde el cual se aplica. No se permite el bloqueo retroactivo.

Si un certificado contiene información acerca de una tercera parte, tal parte también puede solicitar el bloqueo del certificado.

La Autoridad deberá bloquear los certificados emitidos según lo expresado en el Articulo 4, párrafo 5 si un certificador finaliza sus actividades o se revoca su licencia.

Articulo 9: Sello de Fecha y Hora. ➦

Un certificador deberá rotular información digital a pedido con un sello de fecha y hora, siendo aplicable en consecuencia la Sección 5, párrafo 5, sentencias 1 y 2.

Articulo 10: Documentación. ➦

Un Certificador deberá documentar las medidas de seguridad tomadas para cumplir con esta ley y la Ordenanza Legal según lo expresado en el Articulo 16, como asi también los certificados expedidos de modo tal que la información y su condición de no falsificada se pueda verificar en todo momento.

Articulo 11: Cese de las actividades. ➦

Ante el cese de sus actividades, un certificador deberá notificar de esto a la Autoridad tan pronto como sea posible y deberá asegurar que los certificados validos al momento del cese sean tomados por otro certificador o sean bloqueados.

El certificador deberá transferir la documentación según lo expresado en el Articulo 10, al certificador que tome sus certificados, o si no a la Autoridad.

El certificador deberá inmediatamente notificar a la Autoridad de un procedimiento de declaración de quiebra o procedimientos de ajuste.

(Nota de los Traductores: No se hace mención a la lista de certificados revocados del certificador que cesa sus funciones. No es claro a que se hace referencia con procedimientos de ajuste, en alemán "vergleichsverfahrens".)

Articulo 12: Protección de la información. ➦

El certificador puede recopilar información personal solo directamente de la persona afectada y solo en la medida que sea necesario para los propósitos de un certificado. La recopilación de información de un tercero esta permitido solo con el consentimiento de la persona afectada. La información solo puede ser usada para otros propósitos que los descriptos en la sentencia 1 si esta ley u otra reglamentación legal lo permiten, o lo consciente la persona afectada .

En el caso de que el dueño de la clave utilice un seudónimo, el certificador deberá transmitir la información concerniente a su identidad ante pedido de las propias autoridades, en tanto este sea necesario para procesar crímenes o malas conductas, para proteger contra daños a la seguridad pública u orden público, o para cumplir las obligaciones legales de las autoridades de protección constitucional del Gobierno Federal y los Estado Federales, el servicio de Seguridad Federal, servicio de Seguridad Militar o la autoridad de la aduana criminal. Los informes se deberán documentar.

La sección 38 de la Ley de Protección de Información Federal deberá aplicarse, con la condición de que también puede llevarse a cabo una revisión si no hay bases para la previsión de violaciones de la protección de información.

Articulo 13: Control e Implementación de Responsabilidades. ➦

La Autoridad puede tomar medidas con respecto a los certificadores para asegurar el cumplimiento de esta Ley y la Ordenanza Legal. Puede también y, en particular, impedir el uso de componentes técnicos inapropiados e impedir el ejercicio de actividades licenciadas total o parcialmente. Las personas que den una impresión falsa de tener una licencia según el Articulo 4, pueden ser vedadas de ejecutar certificaciones.

Los certificadores deberán permitir a la Autoridad ingresar en su negocio y locales operativos durante las horas normales de negocio con el propósito de supervisar según párrafo 1, sentencia 1 y, a pedido, deberán presentar los libros relevantes, registros, recibos, escritos y otros documentos, para su inspección y deberán proveer la información y asistencia necesarias. La persona requerida de proveer la información puede negarse a proveerla si podría hacerlo pasible a él o a alguno de sus familiares mencionados en el Articulo 383, párrafo 1 a 3 del código de Procedimiento Civil, de prosecución criminal o procedimiento bajo la Ley de Mala Conducta. La persona requerida de proveer la información deberá ser informada de estos derechos.

(Nota de los Traductores: Debe informarse de los derechos antes de requerirle información.)

En caso de no cumplir con las obligaciones acordadas en esta Ley u Ordenanza Legal, o ante el surgimiento de razones para revocar una licencia, la Autoridad deberá revocar tal licencia, si las medidas del párrafo 1, sentencia 2 parecen no dar resultado.

En caso de devolución o revocación de una licencia o cese de la actividad de un certificador, la Autoridad deberá asegurar que tal actividad sea tomada por otro certificador o que los contratos con los suscriptores de clave de firma sean rescindidos. Esto también se aplica respecto a la declaración de quiebra o procedimientos de ajuste, si no se continua con la actividad licenciada.

(Nota de los Traductores: Respecto a procedimientos de ajuste, vale la nota del artículo 11.)

La revocación de la licencia no afecta la validez de los certificados expedidos por un certificador. La Autoridad puede ordenar el bloqueo de certificados si los hechos justifican suponer que los certificados han sido alterados o no son lo suficientemente seguros contra falsificaciones, o que los componentes técnicos usados para la utilización de claves demuestren deficiencias de seguridad las cuales permiten que la falsificación de la firma digital o que la falsificación de la información firmada no sea detectada.

Articulo 14: Componentes técnicos. ➦

Para la generación y almacenamiento de claves de firma y la generación y verificación de firmas digitales, se deberán utilizar componentes técnicos que tengan características seguras que hagan confiablemente detectable la falsificación de firmas digitales y la falsificación de información firmada, y que protejan contra el uso no autorizado de las claves de firma privadas.

Los componente técnicos utilizados para generar firmas digitales deberán permitir que el firmante identifique en forma confiable y previa la información que va a firmar.

Para la verificación de la información firmada, se deberán usar aquellos componentes técnicos que tengan características seguras que permitan determinar que la información no ha sido alterada, a cual información se refiere la firma digital y a cual propietario de la clave de firma se le atribuye la firma digital.

Respecto de los componentes técnicos con los cuales los certificados de clave se mantienen de manera comprobable y accesible según Articulo 5, párrafo 1, sentencia 2, se deberán tomar medidas para proteger los registros de certificado de ser alterados o accedidos sin autorización.

Respecto de los componentes técnicos según párrafos 1 a 3, deberán ser suficientemente examinados con la última tecnología y deberá ser verificado el cumplimiento de los requerimientos por una instancia reconocida por la Autoridad.

Se puede asumir que los requerimientos de los párrafos 1 a 3 concernientes a seguridad técnica, se cumplen para componentes técnicos que están en circulación o que fueron legalmente fabricados de acuerdo con reglas o requerimientos de otro Estado Miembro de la Unión Europea o de otro Estado Firmante del Tratado en el Area Económica Europea, cuando tal Estado garantice el mismo nivel de seguridad. En casos individuales y cuando hay una buena razón, la Autoridad puede requerir una demostración de que los requerimientos del párrafo 1, han sido cumplidos. En la medida que sea requerido que se presente una confirmación de una instancia reconocida por la Autoridad para demostrar los requerimientos técnicos de seguridad dentro del significado de los párrafos 1 a 3, entonces se deberá considerar las confirmaciones por instancias licenciadas en otro Estado Miembro de la Unión Europea o en otro Estado Firmante del Area Económica Europea, si los requerimientos técnicos, verificaciones, y procedimientos de verificación sobre los cuales se basan los registros de tales instancias son equivalentes a las instancias reconocidas por la Autoridad.

Articulo 15: Certificados extranjeros. ➦

Las firmas digitales que se puedan verificar con una clave pública de firma para la cual exista un certificado extranjero de otro Estado miembro de la Unión Europea o de otro Estado firmante del Tratado en el Area Económica Europea son equivalentes a firmas digitales según esta ley, en tanto puedan demostrar un nivel de seguridad equivalente.

El párrafo 1 también se aplica a otros Estados en la medida en que se suscriban acuerdos internacionales relativos al reconocimiento de certificados.

Articulo 16: Ordenanza Legal. ➦

El gobierno federal tiene el poder para promulgar a través de la Ordenanza Legal las disposiciones necesarias para implementar según los Artículos 3 a 15:

Los detalles de los procedimientos para otorgar, transferir y revocar una licencia, así como el procedimiento de cese de las actividades licenciadas;

Las circunstancias que originan honorarios según el Articulo 4 párrafo 6, y el monto de los honorarios;

Los detalles de las obligaciones de los certificadores;

El periodo de validez de los certificados de clave de firma;

Los detalles de la estructura de control sobre los certificadores;

Los detalles de los requisitos de los componentes técnicos, así como la verificación de los componentes técnicos y la confirmación de que los requisitos hayan sido cumplidos;

El plazo en el cual debería comenzar a usarse una nueva firma digital, así como los

procedimientos asociados.