Los Prestadores de Servicios de Certificación de Firma Electrónica en el Derecho Chileno*

Raúl Arrieta Cortés
Abogado. Asesor en Tecnologías de la Información
y Comunicaciones, Ministerio de Economía.

SUMARIO: Introducción.- I.- Los prestadores de servicios de certificación.- II.- Obligaciones de los certificadores.- Obligaciones comunes a ambos tipos de certificadores.- Obligaciones exclusivas de los certificadores acreditados.- III.- Actividades que realizan los prestadores de servicios de certificación.- Actividad de certificación.- Actividad de homologación.- IV.- Certificados de firma electrónica.- Menciones básicas del certificado de firma electrónica.- Límites funcionales del certificado de firma electrónica.- Tipos de certificados en la ley de firma electrónica.- V.- Responsabilidad de los certificadores.- Seguro de responsabilidad civil.- Intervención de notarios y oficiales del Registro Civil.- VI.- Acreditación de los prestadores de servicios de certificación.- Problema de nomenclatura. Diferencia con otros sistemas de acreditación.- Procedimiento de acreditación de los prestadores de servicios de certificación.- Término de la acreditación.- Procedimiento de cancelación de la acreditación.- Publicidad de la cancelación de la inscripción de la acreditación.-

INTRODUCCIÓN.

En los últimos años, como consecuencia de la Sociedad de la Información,[1] han surgido una variada gama de figuras que interactuan con la finalidad de permitir la generación, procesamiento y distribución del conocimiento y de la información.

Es en ese escenario que surgen los prestadores de servicios de certificación, cuya función principalmente es la de expedir certificados de firma electrónica.

* Trabajo elaborado sobre la ponencia pronunciada en el *"Seminario Firma Electrónica en Chile. Ley 19.799"*, organizado por el Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, entre los días 24 de junio y 22 de julio de 2002.

[1] Sistema económico y social donde la generación, procesamiento y distribución del conocimiento e información constituye la fuente fundamental de productividad, bienestar y poder. Mensaje de la Ley 19.799, pág. 1.

Es importante hacer presente que los prestadores de servicios de certificación en el derecho comparado han recibido diferentes denominaciones, tales como terceras partes confiables o autoridades de certificación. No obstante, sin importar el nombre que reciban, siempre realizan esencialmente la misma función: emitir certificados de firma.

I. LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN.

La Ley 19.799, de firma electrónica, define al certificador o prestador de servicios de certificación, en el artículo 2 letra c, disponiendo que es "la entidad prestadora de servicios de certificación de firmas electrónicas".

Dicha definición no ayuda al lector a esclarecer lo que es un prestador de servicios de certificación; sin embargo, se encuentra complementada por lo preceptuado en el artículo 11 *ejusdem*, el que, siguiendo la directiva europea sobre firma electrónica,[2] distingue entre certificadores acreditados y los que no lo están.

Los prestadores de servicios de certificación son las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorgan certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar. Estas personas jurídicas, en caso que deseen acreditarse, deberán estar domiciliadas en Chile y seguir el procedimiento de acreditación que señala el Título V de la ley y que desarrolla el Reglamento.

De la definición señalada se puede sostener que:

1. *Se trata de personas jurídicas.* El desarrollo de la actividad se encuentra reservado a este tipo de personas y consecuentemente la actividad les es privativa. Luego, jamás una persona natural podrá actuar como certificador de firmas electrónicas.
2. *Nacionales o extranjeras.* No es necesario que la persona jurídica se encuentre domiciliada en Chile para prestar los servicios de certificación de firma electrónica. Sin perjuicio de ello, sí es requisito domicilio chileno, para acreditarse y poder prestar el servicio como corresponde.
3. *Públicas o privadas.* Las personas jurídicas pueden serlo de derecho público o de derecho privado y, consecuentemente, nada obsta a que el certificador adopte cualquiera de las formas sociales previstas en el ordenamiento jurídico o, como así también, que el Estado cree una empresa para que desarrolle tal actividad.

[2] Directiva 1999/93/CE de 13 de diciembre de 1999.

II. OBLIGACIONES DE LOS CERTIFICADORES.

La obligación es el vínculo jurídico entre dos o más personas determinadas (titular del certificado y prestador de servicios de certificación), mediante el cual una de ellas, el acreedor, tiene la facultad de exigir algo de la otra, llamada deudor.

La ley ha creado dos categorías de prestadores de servicios de certificación, aquellos que están acreditados y los que no lo están. Como consecuencia, se hace necesario analizar las obligaciones que deben cumplir ambas entidades, distinguiendo entre las obligaciones que son comunes y las que son exclusivas de los prestadores acreditados de servicios de certificación.

Obligaciones comunes a ambos tipos de certificadores.

1. Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano (artículo 12 a) de la Ley).[3]

   Esta primera obligación que se impone a los prestadores de servicios de certificación, conlleva un doble carácter:

   a) Tener prácticas de certificación que sean objetivas y no discriminatorias.

      Las prácticas de certificación son una descripción detallada de las políticas, procedimientos y mecanismos que el certificador se obliga a cumplir en la prestación de servicios de certificación u homologación (artículo 6 Reglamento).

      Sobre la base de lo anterior, podemos afirmar que se trata de una declaración unilateral que hace el prestador de servicios de certificación por medio de la cual, se obliga a desarrollar la actividad de certificación y homologación en la forma descrita en la práctica. En tal sentido, se trata de fuente de obligaciones para el certificador, las que pasan a ser parte integrante del contrato que suscribe el titular del certificado de firma electrónica con la entidad que se lo provee.

      El que sean objetivas y no discriminatorias será una cuestión de hecho que deberán resolver, caso a caso, los Tribunales de Justicia.

   b) Comunicarlas a los usuarios de manera sencilla y en idioma castellano. Nos encontramos en presencia de una declaración unilateral de voluntad, extremadamente técnica, que pasa a formar parte integrante del contrato, entre certificador y titular de firma electrónica. El legislador estimó necesario para proteger a la parte más débil de la relación (titular del certificado) que el certificador tenga la obligación de entregar al usuario una información simple y comprensible.

[3] Esto es lo que técnicamente se conoce con el nombre de CPS por su sigla en inglés que abrevia *"certification practice statemen"*.

Sólo de esa manera, el usuario podrá elegir con libertad y responsabilidad, al momento de tomar la decisión de adquirir una firma electrónica.

En cuanto al idioma, pese a que se trata de una actividad que se desarrolla en el marco de Internet, en Chile, el castellano es el idioma oficial y consecuentemente, las actividades que se realizan en el territorio nacional, deben permitir a los habitantes conocer las condiciones en que se realizan en la lengua oficial.

2. Mantener un registro de acceso público de certificados, en el que quedará constancia de aquellos emitidos y los que queden sin efecto, en los términos señalados por el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para este efecto, los que no se podrán utilizar para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la Ley N°19.628, sobre protección de la vida privada.

   Esta obligación también conlleva un doble carácter:

   a) Registro de acceso público de certificados. Se traduce en la necesidad del certificador de contar con un sitio de acceso electrónico, en el que se contenga un listado de los certificados de firma electrónica que ha emitido, indicando si el certificado se encuentra vigente o revocado.

      Con ello, la Ley ha modificado la estructura tradicional en que se conservan estas listas, en la experiencia nacional e internacional, toda vez que ellas son únicamente listas de revocación, que no muestran los certificados que se encuentran vigentes, sino los que han sido revocados o suspendidos. En consecuencia, la vigencia de un certificado de firma electrónica se determina por exclusión, ya que al no encontrarse el certificado de firma electrónica en dicha lista hace presuponer que está vigente.

      Dicho registro debe permitir el acceso en forma regular y continua, lo que deberá ser descrito en las prácticas de certificación y calificadas por los Tribunales de Justicia, en caso de conflicto.

   b) Conservación de datos. Los antecedentes que proporcione el solicitante del certificado, para la contratación del mismo, deben ser conservados por el prestador de servicios de certificación, por al menos seis años.

      Es interesante advertir que, frente a esta obligación, el legislador nada señaló en relación a lo que ocurre en caso que el prestador de servicios de certificación cese en su función. Al respecto, estimamos que donde no distinguió el legislador no corresponde hacerlo al intérprete y, en consecuencia, la obligación se mantiene para el certificador aun cuando deje de desarrollar la actividad. El mismo criterio

siguió el Reglamento de la Ley, cuyo artículo 11 inciso 2°, dispone que, en caso que el prestador de servicios de certificación cese en su actividad, deberá transferir dichos datos a un prestador acreditado de servicios de certificación o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los seis años desde la emisión de cada certificado.

El objetivo de lo anterior, es garantizar la disponibilidad de los antecedentes que sirvieron de fundamento a la emisión de un certificado por todo el tiempo que el legislador estimó que era necesario, a los efectos de poder contar con ella en el evento que se produzca algún conflicto que requiera recurrir a dicha información.

3. En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establece el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

   Uno de los principios inspiradores de la ley, que se encuentra consagrado en el artículo 1, es el de la libre prestación de servicios. Ello trae aparejado que cualquier persona jurídica que cumpla con los requisitos legales y reglamentarios puede desarrollar la actividad, e igualmente dejar de hacerlo.

   Esta obligación contiene varios aspectos importantes que es necesario tener presente al momento de producirse el cese de la actividad por decisión del prestador de servicios de certificación:

   a) Comunicar a los titulares de los certificados que el prestador cesará en la actividad.

      Esta comunicación deberá señalar que el certificador cesará en su actividad y, adicionalmente, manifestar al titular del certificado que tiene derecho a oponerse al traspaso de los datos de éste a otro prestador de servicios de certificación, situación en la cual su certificado será revocado (artículo 8 a) del Reglamento).

   b) Dar el aviso con una antelación de al menos dos meses.

      El plazo fijado por esta norma es absolutamente concordante con lo dispuesto en el artículo 12 g) de la ley, que impone al prestador acreditado de servicios de certificación, la obligación de solicitar a la Entidad Acreditadora la cancelación de su inscripción en el registro público de certificadores acreditados que mantiene con al menos un mes de anticipación a la fecha en que se desea se produzca el cese de la actividad, indicando el destino que dará a los datos de los certificados (artículo 8 a) del Reglamento).

Indudablemente para que el certificador que va a cesar en su actividad, voluntariamente, pueda señalar el destino que dará a los certificados de firma electrónica emitidos por él, es necesario que el titular del certificado, haya o no otorgado autorización al certificador a traspasar los datos a otro certificador.

c) Traspasar los datos de los certificados a otro prestador de servicios de certificación, en caso de no existir oposición del titular.

Este requisito, es consecuencia de la necesidad de asegurar la continuidad en la prestación de los servicios de certificación, no obstante la libertad del certificador para dejar de prestar el servicio para el cual fue contratado. Adicionalmente, puede ser considerado como la fórmula que se da al certificador que cesa anticipadamente de prestar un servicio, para no ser compelido al cumplimiento forzado del contrato de certificación de firma electrónica.

Esta norma conlleva un límite intrínseco, cual es que, en caso que el certificador que cesa en la actividad se encuentre acreditado, los datos de los certificados de firma electrónica avanzada que haya emitido necesariamente se los deberá traspasar a un prestador acreditado de servicios de certificación (artículo 8 a) del Reglamento).

4. Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, y las leyes N°19.496, sobre Protección de los Derechos de los Consumidores, y N°19.628, sobre Protección de la Vida Privada.

Se trata de una clásica norma de clausura, que tiene por finalidad no hacer taxativa la numeración de las obligaciones previstas en el artículo 12 de la ley.

Obligaciones exclusivas de los certificadores acreditados.

Se trata de obligaciones que los prestadores de servicios de certificación deben cumplir para obtener y mantener la acreditación:

1. Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten.

Se trata de una obligación que tiene por objeto lograr una efectiva simetría de la información, entre el certificador y el usuario o titular del certificado de firma electrónica.

Por medio de ella, se busca proteger el interés público y fortalecer la elección del consumidor, ya que al contratar sobre la base de una buena información, oportuna y completa, le será posible elegir responsablemente el servicio de certificación que estime conveniente contratar.

2. En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la compare-

cencia personal y directa del solicitante, o de su representante legal, si se tratare de persona jurídica.

Esta obligación, es la que impone al prestador acreditado de servicios de certificación, la realización de actividad registral sobre quien solicita un certificado de firma electrónica avanzada, de forma que se garantice, fehacientemente, la identidad del titular.

Esto tiene fundamento en el hecho de que la firma electrónica avanzada permite identificar fehacientemente al titular del certificado, como consecuencia del vínculo que existe entre el firmante y los datos de creación de firma, razón por la cual es la precisión y certeza del proceso por medio del cual se genera ese vínculo que permitirá dar seguridad y garantía de que la persona que dice ser realmente lo sea.

En el derecho comparado, para el desarrollo de esta actividad registral, se contempla la figura de la Autoridad o Entidad de Registro. Sin embargo, ellas no fueron contempladas en la ley nacional debido a que ésta prevé que la comprobación fehaciente de la identidad del solicitante del certificado de firma electrónica avanzada sea realizada por el propio prestador de servicios de certificación, o bien por un Notario u oficial del Registro Civil, para lo cual el solicitante deberá comparecer personal y directamente. Si se trata de una persona jurídica, deberá hacerlo su representante legal.

El Reglamento ordena que la comprobación fehaciente de la identidad del solicitante se realice en conformidad con las normas técnicas.[4]

3. Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores.

Esta obligación tiene por objeto que la Entidad Acreditadora financie la actividad de inspección que debe desarrollar, por mandato del artículo 20 de la ley, cuyo principal objetivo es garantizar a los usuarios de la firma electrónica avanzada la seguridad técnica del sistema.

Comprende, por lo tanto el peritaje que se realice con la finalidad de constatar el cumplimiento de los requisitos y obligaciones legales y reglamentarias, como la sujeción de la actividad a las normas técnicas que se fijan para el desarrollo de la actividad, como son los gastos de carácter administrativo, que genera el sistema para su adecuado funcionamiento.

4. Solicitar la cancelación de su inscripción en el registro de prestadores acreditados, el que es llevado por la Entidad Acreditadora, con una antelación no inferior a un mes antes del cese en su actividad, y comunicar el destino que dará a los datos de los

[4] ETSI TS 102 042 "Policy requirements for certification authorities issuing public key certificates".

certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.

El principio que está subyacente en esta obligación, es que las cosas se deshacen de la misma forma que se hacen. En consecuencia, si el certificador se acreditó para desarrollar la actividad de una determinada forma, debe desacreditarse para dejar de prestar el servicio correspondiente.

Atendida la importancia del servicio que se presta, nada más y nada menos que la de permitir a sus usuarios comunicarse en forma segura por medios electrónicos, es que debe informar si el servicio que está prestando garantiza la continuidad por medio de otro prestador de servicios de certificación, y en caso de ser así con cuál, o bien en caso contrario si los va a revocar.

La norma en comento habla de los "datos de los certificados", aunque en realidad está refiriendo al certificado propiamente tal. La confusión se produce con ocasión de que al transferir el certificado a otro certificador, necesariamente éste deberá emitir un nuevo certificado de firma electrónica con sus datos. Esto se desprende del hecho que la norma concluye señalando que en caso que los datos de los certificados no se transfieran a otro certificador, estos deberán quedar sin efecto.

5. En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere.

   Ésto conlleva una doble obligación:

   a) Comunicar a sus usuarios de la cancelación. Se impone al certificador, en aras de la seguridad del titular del certificado, teniendo concordancia con la forma en que el certificador realiza la actividad y con el hecho cierto de que al tener dicha calificación se encuentra legalmente habilitado para emitir certificados de firma electrónica avanzada. Al ser cancelada la inscripción es revocada la acreditación y, en consecuencia, el certificador pierde la habilitación para desarrollar la actividad como acreditado.
   b) Traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere. Se obliga así al prestador de servicios de certificación, a traspasar los datos de sus certificados a otro prestador, y ello como consecuencia de que han cambiado las circunstancias bajo las cuales contrató el titular del certificado. Este aspecto parte de la base que el certificador al ser desacreditado cesa en el desarrollo de su actividad, lo que no es predeterminable, ya que éste podrá tomar la determinación de seguir desarrollando la actividad sin estar acreditado. En este caso este aspecto de la obligación debe mantenerse restringido al traspaso de los datos de los certificados de firma electrónica avanzada por ellos emitidos, debiendo en consecuencia ser transferidos, necesariamente, a otro prestador acreditado de servicios de certificación.

      En esta forma ha sido tratado en el Reglamento de la Ley (D.S. 181 de 9 de julio de 2002).

6. Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pago.

   Se trata de una obligación que tiene por objeto permitir que la Entidad Acreditadora se encuentre en permanente conocimiento de las circunstancias bajo las cuales el certificador acreditado se encuentra desarrollando la actividad, ello con la finalidad de poder decidir si hay motivo para revocar la acreditación, por haberse modificado las condiciones que sirvieron de base a ella, y atendido el potencial peligro a que se puede ver afectada la comunidad, como consecuencia de las nuevas circunstancias.

III.- ACTIVIDADES QUE REALIZAN LOS prestadores de servicios de certificación.

La Ley 19.799 no contiene norma alguna que señale de una manera categórica cuales son las actividades que realizan los certificadores.

Sin embargo, lo dispuesto en el artículo 11, que define a los prestadores de servicios de certificación, nos permite discurrir que la ley imperativamente les ordena prestar el servicio de certificación. Ello conlleva la necesidad de determinar que se entiende por certificación bajo el prisma de este cuerpo legal.

La norma en comento agrega que el certificador puede prestar servicios adicionales, al disponer "sin perjuicio de los demás servicios que puedan realizar". Esto llevó a un interesante debate parlamentario en torno a la necesidad de que los certificadores fueran personas jurídicas con giro exclusivo, buscando interpretar que dicha expresión, recogida del derecho comparado,[5] trae consigo que el prestador de servicios de certificación puede realizar actividades que no se encuentran dentro del giro del negocio. Sin embargo, ello hubiera sido acorde con la tendencia mundial, toda vez que dicha expresión apunta a la prestación de servicios complementarios que no sólo se encuentran dentro del giro del negocio, sino, lo que es más, permiten que este se

[5] Directiva europea citada, Ley Modelo UNCITRAL para firma electrónica.

desarrolle de una manera más plena, satisfaciendo de esta manera los diferentes requerimientos que pueden tener los distintos actores que comercializan o se relacionan por medios electrónicos y que persiguen que cada vez sea más seguro.

Actividad de certificación.

La certificación de las firmas electrónica buscan generar seguridad para los usuarios, para ello actúan terceras partes en la suscripción de un documento electrónico, firmado por medio de una firma electrónica avanzada, por medio del cual se garantiza que quien hizo uso de los datos de creación de firma, realmente es la persona que se está identificando. En resumen, su labor consiste en actuar asociando los datos de creación de firma de una persona a los antecedentes que recopilaron al momento de registrar al solicitante y, de esta manera, poder permitir a quien recibe un documento electrónico firmado, tener la certeza de que quien dice ser realmente es, en forma fehaciente, dependiendo de la naturaleza de la firma.

Como consecuencia de las diferentes necesidades de los usuarios, en cuanto a la certeza de la identificación que se produce en la red y los costos que la misma lleva asociada, es que el legislador ha previsto la posibilidad de que se certifiquen las firmas electrónicas o firmas electrónicas avanzadas. La diferencia entre ambas radica, desde un punto de vista técnico, básicamente en el grado de certidumbre con que el titular del certificado se puede identificar en la red.

Por lo anterior es que tratándose de un certificado de firma electrónica avanzada, se han impuesto mayores exigencias para la prestación del servicio, ya que la identificación que se hace debe ser fehaciente y, en consecuencia, será fundamental la calidad de registro que se haga del solicitante. Para ello es que se han desarrollado diferentes fórmulas que se explican a continuación:

1. Solicitud del solicitante. La adquisición de un certificado de firma electrónica es un acto voluntario, sin perjuicio de que ciertas circunstancias pueden llevar a que una persona se vea forzada a contar con uno para los efectos de poder insertarse en las diferentes formas de comunicación que se impongan al interior de una determinada comunidad, a la cual pertenezca, o le interese pasar a formar parte.

   Sin embargo, sea cual sea el grado de libertad que tiene la persona para solicitar la firma electrónica, debe realizar un acto voluntario, cual es solicitar que se le emita un certificado de firma electrónica. Para ello, junto con solicitar al prestador de servicios de certificación que se le emita el certificado, deberá proporcionar una serie de antecedentes de carácter personal que dotarán, en parte importante, de contenido al certificado, permitiendo cumplir con posterioridad la función de instrumento identificador en la red.

   Los antecedentes que el solicitante deba declarar dependerán de la naturaleza del certificado que esté solicitando y de lo que señalen las prácticas de certificación del

prestador con quien se esté contratando. Sin embargo, al tenor de lo dispuesto en el artículo 15 letra c) de la ley, al menos deberá indicar el nombre, dirección de correo electrónico y rol único tributario.

En cuanto a los medios o vías por las cuales puede realizarse la solicitud, se deberá estar con lo señalado en las prácticas de certificación. Estimamos, que la solicitud se podrá realizar por cualquier medio, toda vez que la actividad de verificación de los contenidos de la misma se realiza durante el proceso de registro del solicitante.

2. Registro del solicitante. Una vez que el prestador de servicios de certificación recibe la solicitud, debe proceder a la aprobación de la misma, y para ello deberá comprobar los antecedentes que le han sido declarados.

   Los procedimientos de comprobación son fundamentales para que el sistema de las firmas electrónicas funcione en capacidad de brindar confianza a los usuarios y de esta forma puedan tener lugar las comunicaciones electrónicas seguras. Por medio de estos procedimientos, el prestador de servicios de certificación verifica la exactitud de los datos del certificado, que de acuerdo a las prácticas y políticas del prestador de servicios de certificación deben ser verificadas.

   Existen diferentes aspectos a ser verificados, pero siempre será necesario comprobar lo siguiente:

   a) Identidad del sujeto. La comprobación de la identidad del solicitante, es indispensable que se realice en buena forma, ya que es justamente en esta etapa de la emisión del certificado que se da seguridad y certeza de que la persona que se identifica en la red con dicho certificado es realmente quien dice ser.

      Mientras más precisa sea la forma en que se realiza la comprobación de la identidad de la persona, mayor confianza existirá en el certificado y, consecuentemente, menos posibilidades de rechazo del mismo por terceras personas que deben confiar.

      Existen diferentes técnicas para verificar la identidad del solicitante, dependiendo del grado de certeza con que se quiera dotar a la firma electrónica:

      - Presencia personal. Es la forma más segura de verificar la identidad de una persona, toda vez que evita, o al menos se dificulta, la suplantación de personas.

        Consiste en la comparecencia personal del solicitante ante el prestador de servicios de certificación para que realice, en conformidad con las normas técnicas y sus prácticas de certificación, la verificación de la identidad del solicitante.

        El hecho que el certificador realice la verificación de la identidad del solicitante en la forma debida, no obsta a eventuales conductas delictuales por parte del solicitante y que al no ser fácilmente perceptibles pueden hacer incurrir en

un error. Consecuentemente, lo que se persigue es que se utilice la debida diligencia para obtener un resultado certero.

- Documentos acreditativos. Consiste en pedir al solicitante de una firma electrónica que proporcione antecedentes escritos que den fe de su identidad. Habitualmente, se recurre a documentos que han sido emitidos por datarios de fe pública. Por ejemplo, cédula de identidad, pasaporte, declaración jurada de identidad ante Notario.

  Esta clase de documentación permite obtener la información de quien solicita un certificado, sin embargo, no es posible por medio de ella realizar la comprobación fehaciente de la identidad del solicitante, toda vez que, al no cotejar dicha documentación con la presencia física de la persona, puede presumirse que cualquiera pudo obtener dichos documentos y suplantar a quien efectivamente lo es.

- Confirmación de datos personales por una tercera parte. Se trata de mecanismos en los cuales la información que es proporcionada por el solicitante de una firma electrónica, es cotejada por una tercera parte que la coteja con una base de datos que se mantiene para dichos fines. Ejemplo, de estas terceras partes, puede ser DICOM con su sistema de información de personas naturales y jurídicas.

  La utilización de esos sistemas deberá estar en armonía con lo preceptuado en la Ley 19.628 sobre protección de datos personales.

- Sistemas mixtos. Se trata de sistemas que combinan las diferentes técnicas señaladas, de manera de satisfacer de mejor forma las exigencias legales y de mercado.

  En Chile, los prestadores acreditados de servicios de certificación, para comprobar fehacientemente la identidad del solicitante y de esta forma poder emitir firmas electrónicas avanzadas, deberán recurrir a sistemas mixtos, donde la comparecencia personal haya sido exigida de todos modos, por mandato del artículo 12 e) de la ley.

b) Posesión legítima de los datos de creación de firma. Se trata de verificar que los datos de creación de firma son entregados realmente a la persona que solicitó el certificado de firma electrónica.

  Los datos de creación de firma, son el medio que permite al titular de la firma signar un documento en forma electrónica. Al respecto, y haciendo una analogía con el soporte papel, podemos decir que estos equivalen a la tinta del lápiz que permitirá únicamente firmar al dueño del mismo.

  En consecuencia, quien se haga de los datos de creación de firma será quien pueda identificarse en la red con la debida seguridad que otorga el prestador de servicios de certificación.

Por lo anterior es que reviste gran importancia que los datos de creación de firma sean efectivamente entregados a su titular, para lo cual se puede recurrir a diferentes medios, por ejemplo, por medio de una declaración jurada en que se acuse recibo de los mismos.

La forma de verificar la posesión legítima de los datos de creación de firma dependerá del sistema de generación de éstos.

Actualmente existen básicamente dos sistemas:

- Generación de los datos de creación de firma en el entorno del titular de los mismos. En este sistema los datos firmantes son generados en el "hardware" o "software" en que serán utilizados y almacenados.

  La gran ventaja que representa este sistema es que elimina todo problema que pueda traer aparejada la transferencia segura de los mismos. Es así como se produce una mayor confianza en el sistema, ya que ha sido el propio titular el que los ha generado y nunca ha dejado de tener el exclusivo control sobre ellos. Sin embargo, representa el problema de no saber si el sistema en que han sido generados, realmente cuenta con las suficientes garantías.

  Este último aspecto no ha sido abordado por la ley nacional, a diferencia de lo que ocurre con la Directiva Europea sobre Firma Electrónica[6] que señala como requisito de una firma electrónica avanzada calificada que se utilicen dispositivos seguros de creación de firma, lo que necesariamente conlleva que tanto el "hardware" como el "software" que se utilice esté debidamente acreditado.

- Generación de los datos de creación de firma en un sistema central. Se trata de un sistema en que los datos de creación de firma son generados por el prestador de servicios de certificación, por lo que dichos datos deberán necesariamente ser transportados desde el certificador hasta el titular del certificado.

  Consecuentemente, en lo que dice relación con la posesión legítima de los datos de creación de firma por el solicitante, el certificador deberá utilizar mecanismos que permitan dar certeza de ello.

  Persiguiendo dicho fin, el Reglamento de la ley de firma electrónica dispone, en el artículo 31, que en el caso que los datos de creación de firma sean generados por el prestador de servicios de certificación, éstos deben ser entregados al usuario o titular del certificado, de manera de garantizar la recepción de los mismos en forma personal. Para dotar de confianza al sistema y evitar manipulaciones abusivas por parte del certificador, es que la misma norma prohibe al certificador mantener copias de los datos de creación de firma electrónica una vez que estos hayan sido entregados a su titular.

[6] Directiva europea citada.

c) Otra información verificable. Como consecuencia de la estructura de los certificados de firma electrónica y de los requerimientos especiales que puede tener cada titular de firma electrónica, es que se prevé la posibilidad de la inclusión de menciones o atributos adicionales, situación en la cual se hará necesario que el prestador de servicios de certificación constate la veracidad de la misma.

Toda información que se incorpore a un certificado de firma electrónica debe ser constatada, de manera que menciones extraordinarias no alteren la cualidad de instrumento indentificador.

3. Firma y emisión del certificado. Una vez que se ha efectuado el registro del solicitante y se ha verificado la exactitud de los datos proporcionados, el prestador de servicios de certificación procede a emitir el certificado de firma electrónica, firmado por medio de la firma electrónica de la cual es titular.

   El certificado de firma electrónica, es un documento electrónico que se encuentra firmado por el propio prestador de servicios de certificación. Ahondaremos en estos aspectos al analizar los certificados de firma electrónica.

4. Publicación y archivo. Una vez que el certificado de firma electrónica ha sido emitido y firmado por el prestador de servicios de certificación, la ley manda en el artículo 12 que el mismo conste en un registro de acceso público al que se acceda por medios electrónicos.

   Para tales efectos, la ley ha autorizado al prestador de servicios de certificación a tratar los datos del titular del certificado (artículo 12 b)). Asimismo, la obligación de archivo consiste en la mantención de los datos que sirven de base a la emisión del certificado, por un período de a lo menos 6 años, contados desde la fecha de la emisión del mismo.

   La finalidad de la publicación y archivo es hacer que los certificados estén disponibles para la verificación de las firmas electrónicas.

5. Revocación y suspensión. Los certificados de firma electrónica no pueden tener una validez indefinida, muy por el contrario la legislación nacional ha previsto, en el artículo 16 Nº 1, que los certificados tengan un plazo de vigencia, que en ningún caso pueden exceder más allá de 3 años.

   Sin embargo, puede ocurrir que circunstancias como las previstas en la ley o en el reglamento, hagan necesario el término anticipado de la vigencia de un certificado de firma electrónica, temporal o definitivamente.

   La revocación del certificado, de acuerdo al artículo 34 del Reglamento produce el cese permanente de los efectos jurídicos de éste conforme a los usos que le son propios, impidiendo el uso legítimo del mismo. Si el cese es temporal, hay suspensión del

certificado conforme al artículo 33 del Reglamento. Produce los mismos efectos que la revocación, pero en un período de tiempo acotado. Una vez que cesa el motivo que la originó el certificado recobra su valor jurídico, y, en caso que la causa de suspensión se transforme en permanente, el certificado deberá ser revocado.

Actividad de homologación.

La ley dispone en el artículo 15 inciso 2º que los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en la ley y su reglamento, o en virtud de un convenio internacional ratificado por Chile y que se encuentre vigente.

El Diccionario de la Real Academia de la Lengua Española nos dice que homologar es equiparar, poner en relación de igualdad dos cosas. Igualmente, señala que es contrastar una autoridad el cumplimiento de determinadas especificaciones o características de un objeto o de una acción.

En lo que dice relación con la actividad de homologación de certificados de firma electrónica avanzada, lo primero que se debe tener presente es que la homologación de los certificados de firma electrónica avanzada tiene por finalidad evitar que un prestador de servicios de certificación extranjero, que no desea domiciliarse en Chile, tenga que hacerlo para poder emitir dichos certificados.

Lo anterior trae consigo que una persona que no se encuentra en Chile pueda adquirir un certificado de firma electrónica avanzada en el extranjero y celebrar transacciones electrónicas que han de producir efectos jurídicos en Chile con los beneficios probatorios que se consagran en el artículo 5º de la Ley, esto es, que el instrumentos privado signado con firma electrónica avanzado tenga el valor probatorio de los instrumento públicos. Sin ninguna duda esto representa una gran oportunidad de negocios atendido el carácter transfronterizo que presenta el comercio electrónico.

La homologación de certificados de firma electrónica avanzada puede presentar dos formas diferentes en el sistema legal chileno. La primera en virtud de un acuerdo o convenio de homologación entre certificadores y la segunda por medio un tratado internacional ratificado por Chile y que se encuentre vigente.

Cuando es consecuencia de un convenio de homologación entre certificadores, opera por medio de la equiparación que hace el certificador acreditado nacional del certificado que ha sido emitido por el prestador de servicios de certificación extranjero. En consecuencia, lo que

hace el certificador nacional es dar testimonio de que el prestador de servicios de certificación no establecido en Chile cumple con los requisitos y obligaciones legales y reglamentarias para el desarrollo de la actividad en el país en forma acreditada. Como resultado de ello, es que se hace responsable de la actividad de certificación que realiza el certificador extranjero.

El reglamento en el artículo 35 señala que para que pueda tener lugar la homologación de certificados de firma electrónica avanzada en la forma descrita, el certificador acreditado deberá demostrar a la Entidad Acreditadora que los certificados por ella homologados han sido emitidos por prestadores de servicios de certificación no establecidos en Chile que cumplen con normas técnicas equivalentes a las establecidas en el reglamento para el desarrollo de la actividad. No se establece un mecanismo de control *a priori* de la certificadora que va a ser homologada, sino que la responsabilidad que asume el prestador acreditado es tan grande que se ha presumido que no va a poner en juego su prestigio y acreditación por homologar certificados de firma electrónica avanzada que hayan sido emitidos por certificadores que no cumplan con estándares equivalentes a los utilizados por el nacional.

Sin embargo, como una forma de que la Entidad Acreditadora pueda efectuar de una manera eficiente la función de inspección que le otorga la ley, es que el reglamento ha ordenado que la certificadora acreditada una vez que practique la homologación de un certificado o grupo de certificados de firma electrónica avanzada le comunique dentro del plazo de tercero día tal situación, y se publique de inmediato en el registro de acceso público que debe mantener el prestador de servicios de certificación como parte de su actividad.

El reglamento no señala la forma en que se debe realizar la homologación y consecuentemente se deja entregada a la mejor fórmula que puedan encontrar los actores que intervienen en la misma. Con todo, se ha ordenado que declaren en las prácticas de certificación la forma en que ésta va a tener lugar, la que en todo caso deberá ser por certificado o partidas de éstos, y nunca por certificadora.

Finalmente, cuando la homologación se produce en virtud de un tratado ratificado por Chile que se encuentra vigente, la fuente de la homologación de los certificados de firma electrónica avanzada se encuentra en él y, consecuentemente, habrá que estar a los términos que bilateral o multilateralmente hayan sido negociados por los países.

IV. CERTIFICADOS DE FIRMA ELECTRÓNICA.

El certificado de firma electrónica es una certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica (artículo 2 letra b) de la ley).

En consecuencia, se trata de un documento electrónico que da fe de la relación que hay entre el titular de dicho documento y los datos que permiten generarlo.[7]

Del análisis de la Ley se puede advertir que si bien el legislador no adhirió a ninguna tecnología en particular, de manera tal de respetar el principio de neutralidad tecnológico propugnado en el artículo 1º, debió recurrir a la tecnología que mayoritariamente se encuentra disponible en la actualidad, con algunas salvedades conceptuales, a los efectos de redactar la misma. Es por ello que es habitual oír hablar en los medios especializados que la ley de firma electrónica se basa en un sistema de PKI asimétrica. Si bien ello es cierto, por lo expresado, no es del todo exacto, ya que se tomaron las precauciones necesarias para no reducir la Ley a esa tecnología. La razón fundamental de ello es el hecho de que la tecnología avanza de manera más rápida de lo que es posible la adecuación normativa.

Para analizar una firma electrónica avanzada que opera sobre tecnología PKI,[8] haremos algunas precisiones, de manera de instruir al lector no lego en la materia y así hacer más sencilla su comprensión.

La tecnología PKI es un sistema que utiliza la criptografía para generar un sistema de cifrado de llave pública.

Actualmente es posible distinguir entre criptosistema simétrico o de llave secreta y asimétrico o de llave pública.

Un criptosistema, es un conjunto normativo constituido por un emisor de información, que genera un mensaje denominado mensaje en claro; un dispositivo cifrador (que eventualmente incluirá un generador de claves), que con el concurso de una clave criptográfica, o simplemente llave de cifrado, transforma el mensaje claro en un mensaje ininteligible, denominado texto cifrado; un canal (de almacenamiento o transmisión); un dispositivo descifrador, cuya misión es la inversa del cifrador; y un receptor de la información. Así mismo, debe incluir un protocolo de intercambio de claves.[9]

Históricamente apareció primero el criptosistema simétrico, caracterizado por el hecho de que la llave de cifrado es la misma que se emplea para descifrar. La vulnerabilidad del sistema depende del mantenimiento en secreto de la llave empleada. Ello obliga a que el canal que se utilice para poner la llave en poder del receptor del mensaje sea extremadamente seguro, ya que de ser obtenida por un posible interceptador el mensaje queda al descubierto.

[7] El documento electrónico es toda representación de un hecho, imagen o idea que ha sido creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior. Artículo 2 d) de la Ley 19.799.

[8] También llamada firma digital.

[9] RIBAGORDA GARNACHO, Arturo. *"Sistema de certificación: la firma y el certificado digital"*.

Esto llevo a Diffie y Hellman, en 1976, a demostrar la posibilidad de construir un criptosistema que no precisaba la transferencia de una clave secreta entre el emisor y el receptor del mensaje, con anterioridad a una transmisión cifrada.

Estos criptosistemas asimétricos funcionan sobre la base de dos llaves, una pública que se hace de general conocimiento y una privada que se debe mantener bajo control exclusivo. Obviamente ambas llaves no son independientes, pero del conocimiento de la pública no es posible inferir la privada, a no ser que se tenga algún dato adicional, que también debe mantenerse en secreto o bien debe destruirse una vez que ha sido generado el par de llaves, o bien que se disponga de recursos innumerables y tiempo ilimitado para abocarse al descubrimiento de ellas. Al no ser claves independientes, lo que hace una, lo deshace la otra, o lo que es lo mismo, lo que cifra una llave lo descifra la otra.

Como puede advertirse de la sola lectura, este sistema criptográfico de llave pública, resuelve el problema del canal seguro para la distribución de las llaves, toda vez que la llave pública debe ser conocida universalmente, para que cualquier pueda remitir información cifrada al propietario del par de llaves.

Dos son los principales inconvenientes que tiene este sistema asimétrico. En primer lugar, en lo que respecta a la necesidad de garantizar la autenticidad de las claves públicas, es decir, que la llave realmente pertenece a quien dice ser. En segundo lugar, los cifrados de clave pública son mucho más lentos en sus operaciones de cifrado y descifrado. El primer inconveniente es soslayado por medio de la utilización de prestadores de servicios de certificación, que den fe de la llave pública del destinatario de un mensaje. En relación al segundo inconveniente, no es posible resolverlo sino con el avance de la tecnología, por obedecer a una cuestión técnica y no de confianza, en consecuencia lo que se ha hecho es utilizar este sistema de cifrado para informaciones exiguas.

La firma electrónica avanzada opera sobre la base de un sistema criptográfico asimétrico o de llave pública, donde el titular del certificado posee un par de llaves que han sido proporcionadas por un prestador de servicios de certificación, que da testimonio que el par de llaves se encuentran asociadas a la persona que aparece firmando el documento.

Menciones básicas del certificado de firma electrónica.

El artículo 15 de la ley dispone que los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:

a) Un código de identificación único del certificado.

b) Identificación del prestador de servicios de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada.

c) Los datos de la identidad del titular, entre los cuales deberán necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y

d) Su plazo de vigencia.

Al respecto, lo primero que se hace necesario señalar es que las menciones señaladas deben encontrarse contenidas en todos los certificados de firma electrónica, sin distinción de firma electrónica avanzada o la que no lo es. Lo que permitirá distinguir si el certificado ha sido emitido por un prestador de servicios de certificación, es el que se encuentren en el certificado indicados los antecedentes de la acreditación. El hecho que el certificado se encuentre signado por medio de la firma electrónica avanzada del certificador, no da certeza de la acreditación del mismo, ya que nada obsta a que un prestador no acreditado tenga firma electrónica avanzada y ésta la utilice para firmar certificados que emita, lo cual parece ser lo deseable.

Por otra parte, resulta interesante el hecho de que el legislador haya incorporado como una de las menciones de los certificados de firma electrónica el rol único tributario del titular del certificado y del certificador que lo emite, toda vez que se trata de un identificador único, que es utilizado únicamente en Chile, sin entrar en el análisis terminológico de que en Chile el identificador que tiene toda persona es el rol único nacional y no el rol único tributario, ya que este último está asociado a la actividad tributaria.

Con relación al RUT estimamos que se hará necesario interpretar el cumplimiento de dicha mención de una manera progresiva, toda vez que, como analizáramos con anterioridad, a los prestadores de servicios de certificación no se les exige domicilio en Chile, salvo acreditados, y, en consecuencia, no tendrán RUT que incorporar al certificado. La prudencia y el fomento de la actividad en una Red abierta como lo es Internet, nos lleva a concluir que tratándose de certificados de firmas electrónicas no avanzadas, dicho requisito debería ser satisfecho indicando en el certificado que no hay rol único tributario disponible o bien que se trata de otro identificador permanente.

Límites funcionales del certificado de firma electrónica.

El certificado de firma electrónica podrá establecer límites en cuanto a sus posibles usos, conforme a lo preceptuado en el artículo 14 inciso 3º de la ley. Sin embargo, dichos límites deber ser reconocibles por terceros, como condición de validez de los mismos y la responsabilidad del certificador queda circunscrita al uso que ha sido permitido.

Este aspecto fue desarrollado por el reglamento de la ley de firma electrónica, cuyo artículo 29 inciso 2º, señaló que los atributos adicionales que los prestadores de servicios de certificación introduzcan con la finalidad de incorporar límites al uso del certificado no deberán dificultar o impedir la lectura de las menciones señaladas en el artículo 15 de la ley, ni su reconocimiento por terceros.

Con lo anterior, se ha perseguido que no se incorporen menciones a los certificados que limiten el uso de los mismos a comunidades cerradas, toda vez que si bien se deja abierta la posibilidad de ello, la obligatoriedad de lectura de las menciones básicas permitirá siempre identificarse en la Red con ese certificado de firma electrónica. En consecuencia, la limitación funcional estará dada por el uso que se ha permitido, de conformidad con las prácticas de certificación de prestador con quien se ha contratado (artículo 32 del Reglamento) y las condiciones particulares del contrato.

En resumen, la incorporación de límites funcionales a los certificados de firma electrónica debe obedecer a una cuestión contractual entre el certificador y el titular, y no ha una cuestión tecnológica que genere barreras de entrada, que puedan estimular el desarrollo de conductas monopólicas que afecten la libre competencia.

Tipos de certificados en la ley de firma electrónica.

Del tratamiento que se ha hecho en la ley del certificado de firma electrónica podemos afirmar que el legislador ha regulado de una manera directa lo que dice relación con los certificados de firma electrónica de identidad.

El certificado de identidad es un documento electrónico, firmado electrónicamente por un prestador de servicios de certificación, que avala la vinculación de los datos de creación de firma con el titular del certificado.[10]

Con respecto a la titularidad de un certificado de firma electrónica, se presenta la primera cuestión de interés en la ley, toda vez que ésta no señala de un modo expreso que una persona jurídica puede ser titular de una firma electrónica, lo que no significa decir que éstas no pueden celebrar actos o contratos electrónicos por medio de firma electrónica, sino muy por el contrario, ya que esto último es reconocido a texto expreso en diferentes disposiciones de la ley. El problema se presenta con ocasión de los certificados de firma electrónica avanzada, debido a que en el artículo 12 e) de la Ley, se impone como obligación al prestador acreditado de servicios de certificación en el otorgamiento de esta clase de certificados, la comprobación fehaciente de la identidad del solicitante, para lo cual deberá requerir previamente, ante sí o

[10] Ribagorda Garnacho, Arturo. Ob. citada.

ante notario u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal, si se tratare de persona jurídica. En consecuencia, tangencialmente, la ley prevé la posibilidad de que un prestador de servicios de certificación genere un certificado de firma electrónica avanzada para una persona jurídica.

Frente a ello, resulta interesante determinar cuál es la utilidad práctica que puede tener que una persona jurídica cuente con firma electrónica avanzada, toda vez que en el sistema jurídico nacional éstas no pueden actuar sino por medio de su representante legal, lo que traerá consigo la necesidad de que éste también cuente con un certificado de firma electrónica avanzada para actuar en nombre de la persona jurídica. Por lo tanto, la forma de proceder sería que la persona jurídica signe el documento electrónico y simultáneamente lo haga el representante legal, en una suerte de validación de la actuación.

Otra posibilidad, es que en una extensión del certificado de firma electrónica de identidad se incorpore una mención en la que se señale que se está actuando en representación de una persona jurídica, que se especifiquen los poderes, si se requiere de la firma de más de una persona para obligar, etc. Sin embargo, ello podría llevar a que un mismo certificado tenga numerosas extensiones, ello sin pensar en que una misma persona puede ser representante de más de una persona jurídica. Adicionalmente, es necesario preguntarse qué ocurre si el titular del certificado deja de ser representante legal de la persona jurídica, o sus poderes son modificados, etc. Acarrearía la revocación del certificado de firma electrónica y generaría le necesidad de adquirir un nuevo certificado para que la persona jurídica pueda seguir actuando por medios electrónicos con firma electrónica.

Con la finalidad de resolver los problemas señalados precedentemente es que se han desarrollado los certificados de firma electrónica de atributos, los que si bien no están contemplados en la ley nacional, se encuentran completamente ajustados a la misma y podrían, eventualmente, ser considerados como uno de aquellos "demás servicios que puedan realizar" los prestadores de servicios de certificación que señala el artículo 11 *ejusdem*.

Los certificados de atributos son un documento electrónico firmado electrónicamente por un prestador de servicios de certificación, que avala la capacidad de actuar en nombre de una persona jurídica, con determinados poderes, etc. Su contenido dependerá de la necesidad de proporcionar información del titular, y siempre requieren del acompañamiento de un certificado de firma electrónica de identidad, sin el cual no tienen virtud alguna. En consecuencia, la persona se identifica por medio de su certificado de firma electrónica, el que puede acompañarse de uno de atributo, que indica, por ejemplo, que se está identificando para actuar en nombre de tal o cual empresa y con tales o cuales poderes.