Tecnología Informática

La Tercera Parte Confiable en la Firma Digital.

Por el Dr. Raúl Alejandro Farías

En mis anteriores artículos les hablé sobre los procesos computacionales que intervienen en la firma digital. Vimos que nuestra ley 25.506 otorga eficacia jurídica (art. 1) a la firma electrónica (art. 2) y a la digital (art. 5) de documentos digitales (art. 6), ya se trate de un mensaje de correo electrónico, contrato o transacción on-line.

Viene bien recordar que el éxito del sistema Asimétrico de Clave Pública, en el cual se basa actualmente la firma digital, depende de: A) garantizar que ese complejo algoritmo matemático llamado “clave privada”, propio de cada persona y que se usa para firmar, sea conocida exclusivamente por su propietario y B) que su clave publica pueda ser conocida por todos sin que hubiera lugar a que se generase algún tipo de caos entre las diversas claves públicas de todos los individuos.

El primer caso se resuelve con el uso de tarjetas “chip” o inteligentes que guardan la clave privada, la cual a su vez está protegida por una clave de acceso alfanumérica o pin que solo el propietario de ella conoce. Aunque menos seguros que la anterior, aun es posible guardarla en los soportes magnéticos u ópticos tradicionales, protegiéndolas de idéntica forma. En el segundo caso la solución está dada por el uso de los Certificados Digitales, los cuales básicamente son credenciales o documentos de identidad digitales que vinculan una clave pública con los datos que determinan la identidad de su propietario.

La Tercera Parte de Confianza

El elemento fundamental para la total aceptación de esta tecnología por parte del público y su consecuente uso, está dada por la confianza que se ponga en la autenticidad de los certificados digitales así como la de los datos consignados en ellos, ya que la primera pregunta que le surgirá a la persona que reciba un mensaje firmado de alguien con quien no ha tenido relación previa es: Cómo estoy seguro que quien firma es quien dice ser? La respuesta está contenida en el Certificado Digital en el que se consignan los datos del firmante. Ahora bien, este certificado es auténtico o falso? Es a partir de estas preguntas donde cobra importancia la TPC, Tercera Parte de Confianza (en inglés *TTP, Trusted Third Party*).

La función de TPC la desempeña el **Certificador Licenciado** (CL), quien recibe dicha licencia del ente licenciante, órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y supervisar su actividad. En nuestro país el ente licenciante funciona en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI).

Conforme nuestra ley, los Certificadores Licenciados son personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente administrador para actuar como proveedores de servicios de certificación. La normativa asimismo prevé la existencia de Autoridades de Registro (AR) que son entidades en las cuales el certificador licenciado delega la función de validar la identidad y autenticación de los datos de los titulares de certificados. Asimismo tienen a su cargo archivar y conservar toda la documentación respaldatoria del proceso de

validación de identidad. Este es el lugar que, eventualmente, ocuparán los colegios y asociaciones profesionales, cámaras de comercio etc. Sin perjuicio de ello, los Certificadores Licenciados también pueden desempeñarse como Autoridad de Registro.

Esta es la estructura que en nuestro derecho conforma la Tercera Parte de Confianza. Su objeto, en definitiva, consiste en que aquellos individuos que no se conocen entre sí, conozcan y tengan confianza en un tercero que conoce a ambos y obra de nexo y aval a la vez, garantizando con su propia firma digital inserta en los certificados digitales que emite, que tanto esos certificados como los datos que contienen son auténticos.

En nuestro país la ONTI aun no ha otorgado licencia a ningún proveedor de servicios de certificación público o privado. No obstante las empresas y organismos que se licenciarán en el futuro ya emiten certificados digitales que se pueden obtener a través de sus sitios en Internet. En ese sentido aconsejo al lector que ingrese en “http://ca.sgp.gov.ar/eMail”, sitio de la Autoridad Certificante de la Subsecretaría de la Gestión Pública, para gestionar y obtener en forma gratuita su propio certificado digital para correo electrónico, el cual le permitirá enviar e-mail con firma digital.

En el resto del mundo, son muchas empresas privadas de reconocida trayectoria y prestigio, así como instituciones y organismos públicos que desde hace tiempo se encuentran habilitadas para emitir certificados digitales y operar como TPC conforme a sus respectivas legislaciones. En España, por ejemplo la “Fabrica Nacional de Moneda y Timbre - Real Casa de La Moneda”, a través de CERES (Autoridad Pública de Certificación Española) es proveedor de

Servicios de Certificación digital, emitiendo certificados digitales que permiten a la Administración, empresas y ciudadanos españoles realizar una enorme variedad de trámites en forma segura por Internet .

La elección es nuestra.

El hecho que las licencias sean otorgadas por la ONTI y que esta a su vez disponga de un sistema de auditoría encargado de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados, no evitará que existan terceras partes más y menos confiables. Seremos entonces los propios usuarios quienes elijamos un CL para confiarle los datos de nuestra identidad y confiar en sus certificados. Para ello deberemos estar alertas y no otorgar ligeramente nuestra confianza a cualquier Certificador Licenciado sin antes haber evaluado cuidadosamente su experiencia, antecedentes, infraestructura física, prestigio e idoneidad. Solo así, podremos aprovechar plenamente los beneficios que nos depara el uso de la Firma Digital.

Firmado digitalmente por Raúl Alejandro Farías
Nombre de reconocimiento (DN): CN = Raúl Alejandro Farías, O = Política de Certificación de Correo Electrónico, OU = Persona no verificada - No amparado bajo el Decreto 427/98 de la IFDAPN
Motivo: Artículo creado por Dr. Raúl A. Farías para "Sintesis Forense"
Ubicación: San Isidro, Pcia. de Buenos Aires
Fecha: 2004.10.07 00:14:18 -03'00'