CRIPTOLOGÍA NOTARIAL. Proyectos y riesgos actuales

PROSPECTIVA DE LA FE PÚBLICA DIGITALIZABLE

Dr. (PhD) Ing. Miguel Ángel Gallardo Ortiz, perito criptólogo en www.cita.es

y Avv. Achille Campagna, notario en San Marino, por asociación APEDANICA

Índice:

En 1977, el algoritmo RSA (su nombre se debe a las iniciales de sus inventores Rivest, Shamir y Adleman) revolucionó la informática y las comunicaciones digitales al ofrecer una certificación matemática de la procedencia de un mensaje, o firma digital, con autenticidad e integridad, y opcionalmente, confidencialidad para dirigir el mensaje a un único destinatario,

Casi 40 años después, el desarrollo normativo internacional ha posibilitado el uso de certificados digitales para firma electrónica en prácticamente todo el mundo, con decididos apoyos de las Naciones Unidas y la Comisión Europea que deben inspirar proyectos tecnológicos internacionales para ofrecer nuevos servicios, algunos de ellos inimaginables hasta hace muy poco, y también afrontar riesgos en materia de seguridad criptológica. La firma digital o “digifirma” del notario posibilita mucho más con los mismos riesgos actuales.

En España[1], el artículo 108.1 párrafo 2.º de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, establece que todos los notarios y registradores de la propiedad, mercantiles y de bienes muebles, deben disponer para la adecuada prestación de sus funciones públicas de firma electrónica reconocida. El artículo 110 de dicha Ley dispone que mediante el uso de la firma electrónica podrán remitirse documentos públicos notariales, comunicaciones, partes, declaraciones y autoliquidaciones tributarias, solicitudes o certificaciones por vía electrónica por parte de un notario o registrador de la propiedad, mercantil o de bienes muebles dirigidas a otro notario o

[1] Todas las comunicaciones que deban realizar los notarios y registradores de la propiedad, mercantiles y de bienes muebles a la DGRN se realizarán por medios electrónicos Instrucción de 25 de octubre de 2016, de la Dirección General de los Registros y del Notariado, sobre utilización de medios electrónicos en las comunicaciones de notarios y registradores con la Dirección General de los Registros y del Notariado. (BOE núm. 268, de 5 de noviembre de 2016). Véase http://www.economistjurist.es/actualidad-juridica/legislacion/todas-las-comunicaciones-que-deban-realizar-los-notarios-y-registradores-de-la-propiedad-mercantiles-y-de-bienes-muebles-a-la-dgrn-se-realizaran-por-medios-electronicos/

registrador, a las Administraciones públicas o a cualquier órgano jurisdiccional, siempre en el ámbito de su respectiva competencia y por razón de su oficio. Recientemente[2], la Instrucción de 25 de octubre de 2016, de la Dirección General de los Registros y del Notariado, sobre utilización de medios electrónicos en las comunicaciones de notarios y registradores con la Dirección General de los Registros y del Notariado. (BOE núm. 268, de 5 de noviembre de 2016) establece nuevas obligaciones pero también posibilita innovación notarial en criptografía aplicada al ámbito comercial y mercantil más actual.

En Europa[3], *la seguridad de los sistemas de identificación electrónica es esencial para la confianza en el reconocimiento transfronterizo recíproco de los medios de identificación electrónica. En tal sentido, los Estados miembros deben cooperar en relación con la seguridad y la interoperabilidad de los sistemas de identificación electrónica en el plano de la Unión. Toda vez que los sistemas de identificación electrónica puedan requerir el empleo de equipos o programas informáticos específicos por las partes usuarias a escala nacional, la interoperabilidad transfronteriza exige que los Estados miembros no impongan tales requisitos y los costes asociados a las partes usuarias establecidas fuera de su territorio. En tal caso, se deben debatir y desarrollar soluciones adecuadas dentro del ámbito de aplicación del marco de interoperabilidad. Sin embargo, resultan inevitables los requisitos técnicos derivados de las especificaciones intrínsecas de los medios de identificación electrónica nacionales (por ejemplo tarjetas inteligentes), que pueden afectar a los titulares de esos medios electrónicos*.

En la Organización de las Naciones Unidas (ONU), la resolución[4] aprobada por la Asamblea General [sobre la base del informe de la Sexta Comisión (A/56/588)] 56/80. propone una Ley Modelo sobre las Firmas Electrónicas, de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. En esa resolución de la ONU, que tenazmente inspira las normativas de países distintos y distantes, en todo el mundo, puede leerse:

Observando que un número creciente de transacciones comerciales internacionales se realizan por el medio de comunicación habitualmente conocido como comercio electrónico,

---

[2] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-10201

[3] REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE https://www.boe.es/doue/2014/257/L00073-00114.pdf

[4] http://www.un.org/es/comun/docs/?symbol=A/RES/56/80

en el que se usan métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel…

Artículo 1 Ámbito de aplicación
La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto de actividades comerciales . No derogará ninguna norma jurídica destinada a la protección del consumidor.

Artículo 2 Definiciones
Para los fines de la presente Ley:
a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;
b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;
c) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;
d) Por "firmante" se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa;
e) Por "prestador de servicios de certificación" se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;
f) Por "parte que confía" se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

PROYECTOS INNOVADORES EN CRIPTOLOGÍA NOTARIAL

La tecnología disponible actualmente posibilita la certificación notarial de la autenticidad, integridad, certificación de la procedencia verificando firmas digitales y opcionalmente la confidencialidad de la información criptografiada. Lamentablemente, la inmensa mayoría de los notarios se limitan a utilizar programas o aplicaciones convencionales para digifirmar documentos PDF, y muy excepcionalmente, otros formatos ofimáticos. Muy pocas veces se digifirman fotografías o documentos audiovisuales o multimedia o "metadatos" en notarías.

La Asociación APEDANICA[5], constituida en España en 1992 y registrada en el Ministerio del Interior en 1993, está trabajando en ambiciosos proyectos de firma digital notarizada para telefonía móvil celular en sistemas Android de Google y iPhone de Apple para smartphones[6] .

La idea de APEDANICA es simple y fácil de aplicar para notarios admitan algo más que documentos PDF para su digifirma, porque cualquier archivo en cualquier formato electrónico es firmable electrónicamente por un notario, incluyendo también contenidos audiovisuales.

Así, APEDANICA investiga en técnicas avanzadas para la estructuración de contenidos complejos, como pueda serlo todo lo que almacena un smartphone o un gran centro de proceso de datos cuyas copias de seguridad completas deban ser aseguradas y preservadas con las máximas garantías posibles. Por grandes y complejas que sean las estructuras abstractas de datos, en teoría, en cada caso existe una manera óptima de representarlos fielmente, y una vez representados, pueden ser digifirmados por un notario capaz. Por una parte, el mundo de rastros y relaciones de un smartphone y por otra todo el contenido de un gran centro de proceso de datos, puede ser notarizado devolviendo al interesado una copia total firmada y restituible en un sistema equivalente tantas veces como se desee con la fe pública notarial verificable. Opcionalmente el notario puede dar al interesado una copia también digifirmada pero dentro de un sobre o embalaje precintado de tal manera que siempre pueda garantizarse que el soporte guardado bajo precinto legal no se ha alterado desde que salió de la notaría, pero está bien disponible en cualquier momento para las autoridades. Y además, el notario puede custodiar con su propio protocolo una copia más.

APEDANICA puede colaborar con cualquier notario de cualquier lugar del mundo que desee practicar la digifirma, como prueba preventiva o anticipada, de documentos digitales heterogéneos con máximas garantías criptológicas disponibles actualmente, promoviendo no solamente la certificación, sino también la criptoanalítica pericial para la verificación de las firmas. La experiencia demuestra que muchos documentos que el sistema LexNet

[5] Datos registrales oficiales de APEDANICA en www.cita.es/apedanica.pdf
[6] Véase HABEAS SMARTPHONE, HABEAS AUDIO Y HABEAS DATA PROBÁTICA CRIMINALÍSTICA EN TELEFONÍA CELULAR AVANZADA Y SU ESPIONAJE en http://www.cita.es/habeas-smartphone.pdf y también www.cita.es/apedanica-audiovisual.pdf

considera firmados digitalmente no están debidamente certificados y pueden ser impugnados mediante un dictamen pericial criptoanalítico capaz de conseguir nulidad de actuaciones frente a demandas y querellas mal digifirmadas. El Poder Judicial debería estar preparado para ello.

RIESGOS ACTUALES EN LA CRIPTOLOGÍA NOTARIAL

Metafísicamente, la seguridad no existe. Lo que sí que existe es la inseguridad y lo que se detecta en criptología analítica o criptoanálisis es la violación de una medida de seguridad y, anticipadamente, ciertas vulnerabilidades de sistemas tecnológicos de cualquier clase. En principio, el riesgo de la firma digital de un notario es el mismo que si fuera procurador o abogado, o el que corre cualquier otro usuario con la misma aplicación y certificación. La (in)seguridad de los algoritmos matemáticos empleados en la certificación y firma digital no solamente no es absoluta, sino que ya se conoce un algoritmo capaz de romper el RSA. Desde 1995 Peter W. Shor ha propuesto un criptoanálisis basado en computación cuántica[7]. Por otra parte, las revelaciones de Edward Snowden[8] sobre las actividades de espionaje digital masivo de la National Security Agency (NSA) y servicios secretos británicos hacen suponer que un agente de la inteligencia norteamericana es capaz de hacerse pasar por un notario español, o de otros lugares del mundo, impersonando su identidad digital. Más recientemente, hay noticias de que Rusia es capaz de lo mismo, y puede que incluso más. El "hackeo del hacker", en la empresa italiana "HackingTeam", evidenció el riesgo superior[9].

Conclusiones para la especial atención de notarios (y registradores) de todo el mundo:

1ª Los notarios pueden hacer uso de sus certificados digitales para firmar electrónicamente o digifirmar los más diversos contenidos y formatos mucho más allá del uso y costumbre actual incluso en las notarías más innovadoras. Desde el "**HABEAS SMARTPHONE**" ante un notario, hasta la certificación criptográfica del contenido total de un gran centro de proceso de datos hipercomplejo, el notario tiene competencias inexploradas.

---

[7] Peter W. Shor (AT&T Research), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, Journal reference: SIAM J.Sci.Statist.Comput. 26 (1997) 1484 https://arxiv.org/abs/quant-ph/9508027

[8] En junio de 2013 se conocieron documentos que evidenciaban espionaje masivo de la NSA y APEDANICA presentó la querella ante la Audiencia Nacional http://cita.es/querella-nsa agotando todas los recursos judiciales, reforma http://www.cita.es/querella-nsa-reforma y apelación en http://www.cita.es/querella-nsa-apela para que se investigaran. Los hechos y derechos en juego se analizaron en la **tesis doctoral UCM** publicada en http://eprints.ucm.es/33087/1/T36376.pdf

[9] Lo hackedo al "HackingTeam" está publicado en https://wikileaks.org/hackingteam/emails/

2ª Los riesgos de la firma electrónica de un notario son criptológicamente equivalentes a todos los que utilicen la misma tecnología. Por una parte Peter W. Shor y por otra Edward Snowden, representan por sí mismos **ocupación y preocupación criptológica mundial**.

Nota: Este artículo está publicado en
http://www.economistjurist.es/articulos-juridicos-destacados/criptologia-notarial-proyectos-y-riesgos-actuales-prospectiva-de-la-fe-publica-digitalizable/

https://docs.google.com/document/d/1eppNbKsHXRvSO9Wz4LknXZnk1uUscg4WHJyHnBpGNUk/edit

http://www.cita.es/criptologia-notarial.pdf

Más información y actualizaciones:

Dr. (Ph.D.) **Miguel Ángel Gallardo Ortiz**, diplomado en Altos Estudios Internacionales por la **SEI**, ingeniero, criminólogo, licenciado y doctor en Filosofía, perito en informática criminalística y criptología forense, presidente de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA) **Tel. (+34) 902998352**
Fax: 902998379 Twitter @APEDANICA E-mail: miguel@cita.es y **apedanica.ong@gmail.com**