



## EL ALGORITMO RSA PASA A SER DE DOMINIO PÚBLICO

El pasado 6 de septiembre la empresa RSA Security anunció que el algoritmo de clave pública RSA pasaba a ser de dominio público renunciando a sus derechos, permitiendo así que cualquiera pueda crear productos o incorporar en otros el mencionado algoritmo. La patente norteamericana del algoritmo RSA<sup>1</sup>, inventado por Ronald Rivest, Adi Shamir y Leonard Adleman, fue otorgada al Massachusetts Institute of Technology (MIT) el 20 de septiembre de 1983, y transferida en exclusiva a RSA Security Inc. Como todas las patentes, ésta tiene una vigencia limitada que se extinguió el pasado 20 de septiembre de 2000. Sorprendentemente, la terminación de la patente del RSA parece haber causado algún revuelo en los sectores empresariales relacionados con temas de seguridad en las tecnologías de la información.

La posesión de la patente del algoritmo RSA sirvió, en su momento y en Estados Unidos, para montar la empresa RSA Security, dedicada principalmente a desarrollar todo tipo de productos que tuvieran algo que ver con dicho algoritmo. Art Coviello, director ejecutivo de RSA Security afirma que «hacer que el algoritmo RSA sea de dominio público es un paso simbólico en la evolución de este mercado, y creemos que ello afianzará la posición del cifrado RSA como estándar en todas las categorías de aplicaciones y artefactos con o sin cables». Art Coviello también manifiesta que su compañía continuará ofreciendo su librería criptográfica en software RSA BSAFE y que esperan seguir siendo líderes indiscutibles en el mercado internacional de cifrado.

Por otra parte RSA Security ha aprovechado estos 17 años para afrontar problemas reales y publicar sus propuestas de solución en lo que denominaron «Public Key Cryptography Standards», más conocidos por sus siglas PKCS, consiguiendo con ello un liderazgo prácticamente absoluto en el modo de hacer las cosas en el mundillo del desarrollo de aplicaciones y protocolos de la seguridad informática.

### Royalties

El revuelo que se percibe parece estar relacionado con el habitual problema de los *royalties*. Después de liberar al algoritmo RSA de su patente, su antiguo propietario seguirá facturando a sus más de 800 clientes empresariales a través de las licencias de software de la librería RSA BSAFE, y lo hará porque esas compañías no compran el derecho a utilizar un determinado algoritmo, sino una implementación para ellos sólida y probada que les inspira confianza. Sólo un pequeño número de clientes de RSA Security, que únicamente habían obtenido licencia sobre el derecho a utilizar el algoritmo, ya no tienen que seguir pagando por ello.

En la Unión Europea, hasta la fecha, no se

**El pasado 20 de septiembre, el algoritmo criptográfico de clave pública por excelencia, el RSA, dejó de ser propiedad de RSA Security y ya es parte del dominio público. A pesar de ser, en principio, una buena noticia, hay cierto revuelo causado por este tema; ¿cuáles pueden ser sus causas? En este artículo intentaremos echar un vistazo a lo que puede estar ocurriendo en nuestro país y en la Unión Europea que pueda arrojar un poco de luz sobre esta curiosa reacción.**

aceptan ni reconocen patentes para el software ni para los algoritmos matemáticos, ya que la postura tradicional ha sido considerar que los derechos de los artífices de programas de ordenador quedan mejor protegidos bajo las leyes de los Derechos de Autor que como patentes industriales. Sin embargo, la Oficina Europea de Patentes (EPO) y algunos *lobbies* jurídicos muy activos están presionando para que no siga siendo así y la Unión Europea se equipare a la americana y japonesa en lo que a las patentes de software se refiere<sup>2</sup>. La EPO quiere cambiar sus estatutos para permitir que se patente el software y otras creaciones intelectuales como, por ejemplo, patentes sobre «modelos de negocio».

### Ausencia de debate

Lo más curioso y preocupante es que estas presiones se están haciendo sin una amplia discusión pública, política y profesional previa, a pesar de las profundas implicaciones que tendría en el sector informático y de las tecnologías de la información. Es preocupante que la UE pudiese llegar a dar este paso ya que, a fin de cuentas y en una primera aproximación, no sería precisamente ella la que se beneficiase del cobro de tales *royalties* o cánones, ya que el software que se usa hoy en día sigue siendo mayoritariamente norteamericano.

El reconocimiento de patentes de software tal y como se está planteando, podría ir claramente en contra de los intereses de todos los miembros de la UE y, sin embargo, es poca o nula la oposición, e incluso la atención, que están prestando a ello los gobiernos europeos. La única excepción honrosa la encontramos en la Secretaría de Estado Francesa para la Industria que solicita un debate profundo previo antes de modificar tan esencialmente el tratamiento que se hace para la protección legal del software.

Muchos comienzan a hacerse preguntas como: ¿cuál puede ser el interés de estos grupos de presión y por qué llevarlo todo tan «discretamente»? ¿Creen realmente los promotores de esta idea que van a poder patentar algoritmos o procedimientos que inundan prácticamente todas las aplicaciones y desarrollos informáticos y con ello «forrarse»? ¿Se pretenden abrir también en Europa el ejercicio de las «patentes de corso» o los «derechos de pernada» para sacar beneficio a fuerza de querellas judiciales de aquellos que se dedican al desarrollo e integración de sistemas? ¿Quieren iniciar cruzadas probablemente pírricas como las emprendidas en Estados Unidos contra

MP3.com y Napster? ¿Puede llegar a ser el modelo de mercado basado en las tecnologías de la información uno en el que se aplican protecciones o limitaciones al uso de elementos tan esenciales para ese medio como lo son los «hiper-enlaces» (URLs), los GIFs, los MP3 e incluso la futura tecnología WAP<sup>3</sup>?

Quizá la entrega al dominio público de la patente del algoritmo básico sobre el que se han basado en los últimos diez años todas las expectativas de seguridad para el comercio electrónico, para las relaciones con las administraciones y de éstas entre sí, etc., sea un buen ejemplo del desfase que existe entre las dos costas del océano Atlántico. El ejemplo de RSA Security con su famoso algoritmo puede servir para poner de manifiesto, una vez más, que el verdadero negocio, el que genera riqueza, puestos de trabajo, no está en el número y universalidad de las patentes que uno posee, ni en la eficiencia de los abogados que logran recaudar beneficios a fuerza de pleitos, sino en la calidad de los productos que se ofrecen, en la continuidad de servicio, y en la confianza que las empresas logran granjearse entre sus clientes.

Modificar la ley de patentes y aceptar ese tipo de protección para las aplicaciones software que van a construir parte de la realidad social, laboral y empresarial del próximo milenio, es algo que no puede hacerse ni con prisas ni a escondidas. Es mucho lo que está en juego, puede que estemos favoreciendo el cambio de modelo en el mercado europeo y que la riqueza cada día esté menos en «el saber hacer» y en «el hacer», y más en las especulaciones, en «globos llenos de humo», en la narcotizante y efímera fluctuación de índices que cada día significan menos.

Si la protección de los derechos de autor no es suficiente para hacer llegar los beneficios del software a los que lo crearon y a los que invirtieron en su creación, es que las cosas deberían cambiar, pero no sin antes tener en cuenta que la sociedad europea no es, al menos todavía, la misma sociedad que la norteamericana o japonesa, y que las soluciones que allí estén vigentes y parezcan funcionar bien no tienen por qué hacerlo aquí.

En fin; bienvenido sea el algoritmo RSA al Patrimonio de la Humanidad de donde algunos pensamos que nunca debió salir. ●

<sup>1</sup> U.S. Patent # 4,405,829, «Cryptographic Communications System and Method»

<sup>2</sup> ver <http://petition.eurolinux.org/reference/> ó <http://www.freepatents.org>

<sup>3</sup> ver [http://www.oreillynet.com/pub/q/patent\\_list](http://www.oreillynet.com/pub/q/patent_list)