



SOBRE LA GENERACIÓN Y VERIFICACIÓN DE FIRMAS DIGITALES

En los entornos sociales y comerciales la autenticación es la necesidad de probar que son legítimos los mensajes digitales que se comunican y que, consecuentemente, se puede actuar según lo que dicen sin riesgo de que luego las cosas sean distintas. En este caso, la autenticación se entiende como la capacidad de verificar que un mensaje fue realmente originado por el supuesto remitente y que éste no ha sido modificado posteriormente hasta llegar a destino.

La necesidad de autenticación presupone siempre la existencia de la desconfianza y de un oponente o enemigo, que puede ser tanto externo como el propio emisor o receptor del mensaje. El oponente siempre desea que los árbitros o jueces acepten como válidos mensajes que él ha producido y que, por ello, son falsos. La presencia de árbitros y jueces no afecta al éxito o fracaso que pueda tener un oponente externo para subvertir el protocolo de autenticación; eso sólo depende de cuál sea su calidad criptográfica.

Aunque no hay una definición universal de lo que es una «firma», casi siempre se reconoce que ésta satisface una doble función: la identificación del firmante y la expresión -por parte del firmante- del deseo de aceptar el contenido del documento firmado.

- **Identificación del firmante.** La firma, la marca única y particular de cada persona, cuando se aplica sobre un documento permite determinar quién es el autor de ese acto y su presencia física. Los identificadores de un individuo pueden ser de dos tipos: identificadores *intrínsecos* y *extrínsecos*; los primeros son aquellos que son propios de la naturaleza física de la persona¹, mientras que los segundos no son propios del individuo pero que éste los conoce². Una característica de los identificadores extrínsecos es que, una vez exhibidos sus valores concretos, su utilidad como identificador queda comprometida pues deja de ser una información sólo conocida por la persona que se identifica³.

- **Expresión de un deseo.** En nuestra sociedad, el que firma un documento expresa su deseo de ser parte de las consecuencias legales que ese documento implica. Esta característica no es propia de la

Dada la importancia que tiene saber «quién es quién», y «quién se responsabiliza de qué» en nuestras sociedades, es necesario poder estar seguros de la inviolabilidad del sistema social de identificación, en general, y de los esquemas de firma en particular. Así pues, es muy importante determinar qué exigencias han de cumplir la generación y verificación de las firmas digitales que habrán de llegar. Dado el panorama actual en el que se pretende poner en marcha sistemas reales para el comercio, la administración y el juego electrónico, es necesario recoger algunos hechos fundamentales que nos aporten algún criterio para poder estimar la calidad, en cuanto a su seguridad, de las infraestructuras de firma digital que se están proponiendo en estos días.

tecnología del sistema de firma usado, sino que es parte del contexto impuesto por nuestra legislación al modo de uso y aceptación de las firmas, independientemente de la tecnología con las que se generen.

La firma electrónica es una «marca» irreproducible e irrepetible que se adjunta a un documento y que es el resultado de la ejecución de un algoritmo complejo cuyos datos de entrada son de tres tipos:

- (1) datos secretos propios del firmante
- (2) datos relacionados con el contenido y formato del documento en sí y, si nos referimos a la firma con valor legal y comercial, además también hay que incluir
- (3) las identidades públicas del remitente y destinatario.

La firma electrónica, al igual que su homólogo manuscrito, debe requerir, forzosamente, la presencia física del firmante ante el artefacto que computa cada una de sus firmas digitales.

En la actual legislación española⁴ se definen dos tipos de firmas electrónicas, pero la que puede tener interés en escenarios comerciales o administrativos es la denominada «Firma electrónica avanzada»⁵. Un esquema de firma digital es un servicio de seguridad que utiliza un criptosistema asimétrico para definir dos operaciones; la de **Generación de Firma** y la de **Verificación de Firma**, que están relacionadas entre sí de un modo complejo y secreto; conociendo la función de verificación no se obtiene ninguna información sobre cuál es la función de generación⁶. La función de generación de firmas se mantiene en absoluto secreto y sólo puede ser conocida por el titular de la identidad digital que representa. La función genuina de verificación de firmas debe ser públicamente conocida y accesible. Además de estas funciones, un esquema completo de firma digital define el modo de resolver los conflictos que se puedan plantear en general y respecto a la integridad, y la autoría de las

firmas y de los objetos firmados en particular.

El RSA es la base de los esquemas de firma digital que se utilizan hoy en día. Este algoritmo define la existencia de una clave pública y otra privada que se mantiene en el más absoluto secreto por parte del signatario. La «idea feliz» que representa el criptosistema RSA es que conocer los factores de un número puede

convertirse en una tarea computacionalmente imposible si el número es suficientemente grande. Sin embargo, el proceso contrario -la multiplicación de números para obtener su producto- es algo trivial. Para establecer un sistema RSA se eligen en secreto dos números primos de tamaño semejante y con ellos se calculan las claves pública y privada.

La generación de una identidad digital RSA sería aritmética de parbulario si no fuese porque la elección de números primos no es trivial, especialmente si estos han de tener 154 dígitos decimales (512 bits) o más. Cuando los números son de esta magnitud no se puede demostrar su primalidad y hay que usar algoritmos que detectan la presencia de números compuestos; por tanto, no se certifica la naturaleza indivisible de un número sino una cierta probabilidad de que éste no sea compuesto.

Los métodos para la generación de identidades RSA son algoritmos deterministas, por lo que saber con qué valor inicial se ejecutan es equivalente a conocer todo el

1 p. ej.: la cinemática de la firma manuscrita, las huellas dactilares, el timbre de voz, el fondo de ojo, la composición del iris ocular y geometría de las manos, la fisonomía del rostro, etc.)


2 p. ej.: palabras y frases clave, PINs, números de cuentas bancarias, firma manuscrita, datos históricos de la persona, etc.

3 En este grupo de identificadores se incluyen todas aquellas técnicas de comercio telefónico basadas en conjuntos de preguntas que se supone el individuo genuino sabe responder y un impostor no podría (identificación en la banca telefónica, matrices de números, etc.).

4 Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.

5 que la define como «firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos»

6 Algunos ejemplos de sistemas de firma digital los tenemos en los algoritmos RSA y en el DSA.



resultado. La elección del número (semilla) por el que empezar la búsqueda de un factor primo debe hacerse en secreto, al azar y en el instante mismo de iniciar la generación. La disponibilidad en un sistema electrónico de una fuente de números aleatorios exige el uso de una fuente física puesta ahí para tal fin, y no puede obtenerse de ningún parámetro que tenga que ver con el estado del propio autómatas (software).

Según el Real Decreto-ley de firma digital⁷, en su artículo 2f, son cuatro los requisitos que deben cumplir los dispositivos de firma electrónica avanzada, e impone que: (1) la generación de la clave se haga en completo secreto y de forma impredecible, (2) que se utilicen esquemas de firma digital públicamente comprobados, (3) que el secreto que constituye la identidad digital nunca salga del control de su titular, por lo que estamos hablando de objetos físicos de firma digital de fácil custodia ininterrumpida y transporte.

También se exige que el dispositivo no altere, en el sentido de seguir un protocolo

⁷ Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.

⁸ P. ej.: Tarjetas *chip* y llaves USB ahora, PDA's, *hand computers*, teléfonos móviles, etc., quizá en el futuro.

público y estándar, el documento que se va a firmar o del que se va a verificar su firma. El lenguaje que entienden los módulos de firma y los signatarios humanos no tienen por qué ser los mismos, por lo que el Real

La normativa española está hablando de módulos hardware de seguridad aunque no los llame por su nombre; estos artefactos son los únicos que permiten la generación de firmas mínimamente aceptables si se está hablando de una «firma digital avanzada».

Decreto insinúa que el módulo de firma habrá de disponer de un visor que informe de lo que verifica o firma. El visor y el módulo de firma deben encontrarse dentro del mismo perímetro físico y lógico de seguridad.

Así pues, la normativa española está hablando de módulos hardware de seguridad⁸ aunque no los llame por su nombre. Estos artefactos son los únicos que permiten la generación de firmas mínimamente aceptables si se está hablando de una «fir-

ma digital avanzada». Las dos razones básicas para esta única opción están en la generación secreta, confinada e irrepetible de la identidad digital, así como la necesidad que ésta tiene de una buena fuente de números aleatorios. Sin embargo, las cosas no están del todo resueltas ya que también debemos preocuparnos por la verificación de firmas, que obliga a disponer de sistemas físicos de verificación con sus propios visualizadores y teclados para comunicarse con sus propietarios.

La seguridad real que se puede conseguir con esta solución no es tan elevada como muchos fabricantes de *chips* quieren hacernos creer, y en muchas ocasiones la seguridad de los sistemas es prácticamente inexistente si estamos hablando de sistemas avanzados de firma digital, pero ese es un tema que trataremos con detalle en otra ocasión. Por ahora, y aunque parezca mentira, sólo nos falta esperar a que se pongan en marcha las leyes que ya existen para poder hablar de firmas digitales de verdad. |

JORGE DAVILA MURO
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es