



19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 272 963**

51 Int. Cl.:  
**H04L 9/32** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **03715045 .5**

86 Fecha de presentación : **23.01.2003**

87 Número de publicación de la solicitud: **1470663**

87 Fecha de publicación de la solicitud: **27.10.2004**

54 Título: **Procedimiento de generación y verificación de firmas electrónicas.**

30 Prioridad: **24.01.2002 FR 02 00967**

45 Fecha de publicación de la mención BOPI:  
**01.05.2007**

45 Fecha de la publicación del folleto de la patente:  
**01.05.2007**

73 Titular/es: **GEMPLUS**  
**avenue du Pic de Bertagne**  
**Parc d'Activités de la Plaine de Jouques**  
**13420 Gemenos, FR**

72 Inventor/es: **Brouchier, Julien**

74 Agente: **Cañadell Isern, Roberto**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Procedimiento de generación y verificación de firmas electrónicas.

5 El invento concierne un procedimiento de generación y verificación de firmas electrónicas de mensajes electrónicos.

10 El procedimiento del invento se aplica a los sistemas electrónicos en los que un dispositivo emisor o signatario receptor o verificador encargado de comprobar la validez de la firma. La firma electrónica o digital va relacionada generalmente con un mensaje electrónico que se ha enviado, conjuntamente con la firma, al dispositivo verificador. La firma tiene entonces como función autenticar el mensaje y la identidad de su autor.

15 El procedimiento que vamos a describir viene en complemento de los algoritmos de generación y verificación de firmas digitales conocidas, tal como el algoritmo DSA (Digital Signatura Algorithm) descrito en la solicitud de patente US 5,231,668 y anunciado el 30 de agosto de 1991 en el Registro Federal llevado por el US National Institute of Standards and Technology, páginas 42980-42982.

Con objeto de comprender mejor el invento, vamos a recordar lo que es un algoritmo DSA.

20 Como ya se expuso en la solicitud de patente francesa publicada con el n° 2 733 378, una firma DSA está constituida por un par  $\{r, s\}$  de grandes números representados por largas cadenas de cifras binarias (160 cifras). La firma digital se calcula mediante una serie de reglas de cálculo, definidas por el algoritmo, y de un conjunto de parámetros utilizados en dichos cálculos. Por una parte, el algoritmo permite generar firmas, y por otra parte comprobar firmas.

25 La generación de firma DSA hace intervenir una clave privada. La verificación hace intervenir una clave pública que está ligada a la clave privada pero sin ser idéntica a ella. Cada usuario posee un par de claves (privada, pública). Las claves públicas pueden conocerlas todos, mientras que las claves privadas no se revelan nunca. Toda persona tiene la capacidad de comprobar la firma de un usuario utilizando su clave pública, pero solo el poseedor de la clave privada puede generar una firma correspondiente al par de claves.

30 Los parámetros del algoritmo DSA son los siguientes:

- un número primo  $p$ , tal como  $2^{L-1} < p < 2^L$  para  $L$  comprendido entre 512 y 1024 (terminales incluidos), y  $L = 64A$  para un  $A$  entero cualesquiera;
- 35 - un número primo  $q$  tal que  $2^{159} < q < 2^{160}$  y  $p-1$  es un múltiplo de  $q$ ;
- un número  $g$ , de orden  $q$  módulo  $p$ , tal que:  $g = h^{(p-1)/q}$  módulo  $p$ , en donde  $h$  es un entero cualesquiera verificando  $1 < h < p-1$  y  $g > 1$ ;
- 40 - un número  $x$  generado aleatoriamente o pseudoaleatoriamente (es la clave privada);
- un número  $y$  definido por la relación  $y = g^x$  módulo  $p$ ; (es la clave pública); las operaciones modulares definidas a continuación, módulo  $p$  o módulo  $q$  se designarán por mód.  $p$  o mód.  $q$  respectivamente;
- 45 - un número  $k$  generado aleatoriamente o pseudoaleatoriamente, tal como  $0 < k < q$ .

50 Los enteros  $p$ ,  $q$  y  $g$  son parámetros del sistema que pueden publicarse y/o compartirse por un grupo de usuarios. Las claves, privada y pública, de un signatario son respectivamente  $x$  e  $y$ . El parámetro  $k$ , aleatorio, debe generarse de nuevo para cada nueva firma. Los parámetros  $x$  y  $k$  se utilizan para la generación de firmas y deben conservarse secretos.

55 Con el fin de firmar un mensaje  $m$  (que será en general un valor troceado de un fichero inicial  $M$ ), el signatario calcula la firma  $\{r, s\}$  por:

$$r = (g^k \text{ mód. } p) \text{ mód. } q, \quad y$$

$$60 \quad s = (m + xr)/k \text{ mód. } q$$

(en donde la división por  $k$  se entiende módulo  $q$ , es decir que  $1/k$  es el número  $k'$  tal como  $kk' = \text{mód. } q$ ; por ejemplo si  $q = 5$  y  $k = 3$ , entonces  $1/k' = 2$  puesto que  $3 \times 2 = 6$ , ya sea  $1 \text{ mód. } 5$ ).

65 Tras haber testado que  $r$  y  $s$  son distintos de cero, la firma  $\{r, s\}$  se envía al verificador.

## ES 2 272 963 T3

El verificador, que conoce  $p$ ,  $q$ ,  $g$  (ligados a la aplicación),  $y$  (ligado al usuario), y  $m$  (el mensaje que recibió igualmente del órgano signatario), calcula:

$$W = (1/s) \bmod q$$

$$u1 = mw \bmod q$$

$$u2 = rw \bmod q$$

$$v = [g^{u1} \cdot y^{u2} \bmod p] \bmod q$$

Ahora bien, este valor  $\{g^{u1} y^{u2} \bmod p\} \bmod q$  es justamente igual a  $r$  si  $s$  tiene el valor  $\{m + xr\}/s \bmod q$ .

Por consiguiente, el dispositivo verificador recibe  $r$  y  $s$  y verifica que  $v$  es igual a  $r$  para aceptar la firma, o desecharla en caso contrario.

La firma permite a la vez certificar la identidad del signatario (al hacer intervenir una clave privada propia al signatario) y la integridad del mensaje firmado (al hacer intervenir el propio mensaje).

Sólo se garantiza un alto nivel de seguridad si la clave privada permanece secreta con respecto a terceras personas. Ahora bien, existen programas de tipo caballo de Troya, denominados también a veces anti-programas, que bajo la apariencia de programas inofensivos, contienen en realidad funciones ilícitas ocultas destinadas a esquivar los mecanismos de seguridad del sistema informático del órgano signatario con vistas a penetrar por efracción en sus ficheros para consultarlos, modificarlos o destruirlos. Este tipo de programa es entonces capaz de acceder a datos secretos en el órgano signatario, por ejemplo a la clave privada utilizada en el algoritmo DSA.

Para aumentar la seguridad de los sistemas que utilizan firmas electrónicas, ya se conoce la utilización de un código representativo de la máquina física empleada para generar la firma. En particular, el documento EP-A-0 689 316 divulga un procedimiento de firma electrónico, que comprende la generación de una firma digital por un órgano signatario que calcula dicha firma en función de un dato secreto, y la verificación de la firma por un órgano verificador, que verifica si dicha firma cumple con una condición matemática, el órgano signatario recupera, durante la generación de la firma, un código representativo de la máquina física empleada para generar dicha firma, y seguidamente transmite este código a dicho órgano verificador, dicho código generado es independiente del dato secreto, y la verificación consiste además en comprobar si la firma fue generada por mediación de una máquina física habilitada, esta segunda condición se verifica utilizando dicho código enviado por el órgano signatario. Pero este procedimiento no protege el sistema de firma electrónica contra una modificación malintencionada, durante la generación de la firma, que podría aparecer incluso si la firma fue generada por medio de una máquina física habilitada.

Uno de los objetivos del invento consiste en aumentar la seguridad de los sistemas que utilizan firmas electrónicas.

La idea del invento radica en asegurarse no solamente de la validez de la firma electrónica, pero asimismo de la manera como ésta fue generada. Se trata de comprobar, principalmente, si la firma fue generada por medios habilitados por la autoridad que controla el órgano verificador. Por ejemplo, en el caso de una transacción electrónica, se trata de comprobar que la firma electrónica vinculada a la transacción electrónica fue generada por un programa de firma aprobado por la autoridad que administra las transacciones.

Asimismo, según el invento, el órgano signatario suministra al órgano verificador no solamente una firma electrónica, sino igualmente un código representativo del programa empleado para generar la firma. La firma y el código se envían al órgano verificador, el cual verifica su validez.

El invento concierne, así pues, un procedimiento de firma electrónica, que comprende la generación de una firma digital por un órgano signatario que calcula esta firma en función de un dato secreto, y la verificación de la firma por un órgano verificador que verifica si dicha firma cumple una condición matemática, caracterizado porque el órgano signatario calcula además, durante la generación de la firma, un código representativo del programa empleado para generar dicha firma, y después lo transmite a dicho órgano verificador, dicho código generado es independiente del dato secreto, y porque la verificación consiste además en comprobar si la firma fue generada mediante un programa habilitado.

El código constituye un nivel de seguridad suplementario que permite asegurarse que la firma fue generada por medios del órgano signatario habilitados por el órgano verificador.

Según una característica del invento, la verificación de dicha segunda condición consiste en generar en el órgano verificador, mediante un programa idéntico al del órgano signatario, una firma no personalizada establecida tomando como base un dato cualesquiera que reemplaza dicho dato secreto con el fin de obtener el código representativo

## ES 2 272 963 T3

del programa empleado, y en compararlo con el código transmitido por el órgano signatario. La segunda condición se verifica si el código así generado por el órgano verificador y el código transmitido por el órgano signatario son idénticos.

5 El código puede ser generado tomando como base las instrucciones ejecutadas por el programa de generación de la firma.

El invento también tiene como objeto un programa de ordenador de generación y de verificación de firma electrónica destinada a la aplicación de las etapas del procedimiento descrito anteriormente en un ordenador.

10

Por último, el invento tiene como objeto todo soporte de registro, tal como un disquete, disco CD-ROM o memoria, chip electrónico, comprendiendo dicho programa de ordenador.

15

Otras características y ventajas del invento aparecerán cuando se lea la descripción detallada que sigue a continuación y que hace referencia a la figura 1, única, que representa un organigrama del procedimiento del invento en el caso de una generación y de una verificación de firma conformes al algoritmo DSA descrito anteriormente.

20

Según el invento, se ha previsto que el órgano signatario suministre además de la firma digital un código, anotado a continuación CS, que caracterice el programa empleado para generar la firma.

El programa de firma se ejecuta en una máquina física, por ejemplo de tipo PC o Macintosh™, o una máquina virtual, por ejemplo del tipo de aquella empleada en la plataforma JAVA™.

25

Según el invento, el código CS es generado tomando como base las instrucciones del programa de generación de firma, por ejemplo tomando como base el código máquina de las instrucciones de este programa. Evidentemente, para evitar cualquier riesgo de divulgación de los datos secretos (por ejemplo, la clave secreta) contenidos en el programa, se ha previsto seleccionar solamente las instrucciones que hacen intervenir esos datos secretos.

30

En la práctica, en el momento de la ejecución de una instrucción del programa de firma, se testa para saber si contiene datos secretos y después, de no ser así, se memoriza su código máquina o una parte de éste en una memoria no volátil del órgano signatario. Pueden preverse criterios complementarios para determinar las instrucciones que deben almacenarse en la memoria no volátil.

35

También se testan todas las instrucciones del programa para memorizar, en la memoria no volátil del órgano signatario, los códigos máquina de las instrucciones que no comprenden datos secretos. Seguidamente, se tratan estos códigos máquina para formar un código CS representativo del programa empleado para generar la firma electrónica.

40

Preferentemente, se efectúa una operación de troceado en los códigos de máquina registrados. La operación de troceado se realiza mediante una función de troceado. Recordamos que una función de troceado de un número, representado por una cadena de bits, consiste en la producción de una nueva cadena de bits de longitud determinada, longitud diferente o no a la de la cadena inicial, a partir de funciones lógicas ejecutadas en grupos de bits de la cadena inicial. Las funciones de troceado más conocidas son la función SHA y la función MD4. El código obtenido al final de la operación de troceado es el código CS que se enviará al órgano verificador.

45

La operación de troceado permite no solamente codificar el código de las instrucciones memorizadas, sino igualmente elegir la longitud del código al final de la operación. Por otra parte, a semejanza de una huella digital, el código obtenido al final de la operación de troceado depende del contenido de las instrucciones y de sus posiciones en la memoria no volátil del órgano signatario.

50

Como variante, se puede elegir tratar diferentemente los códigos máquina registrados en la memoria no volátil del órgano signatario. Por ejemplo, se puede combinarlos juntos por una operación lógica de tipo O EXCLUSIVO. En esta variante, cada código máquina está combinado con el contenido de un registro del órgano signatario por una operación de tipo O EXCLUSIVO y después de cada operación, el resultado se registra en el registro. El registro se inicializa antes del principio de la primera operación O EXCLUSIVO. Éste se inicializa ya sea a cero, ya sea a un valor particular, por ejemplo el número de identificación del procesador de la máquina en la que funciona el programa de firma. El código CS es el código presente en el registro cuando todos los códigos máquina de la memoria volátil del órgano signatario han sido tratados por la operación O EXCLUSIVO.

60

Estos dos modos de generación del código CS (por una función de troceado o una operación O EXCLUSIVO) sólo se dan como ejemplo. Evidentemente, todos los tratamientos que permiten generar un código CS a partir de las instrucciones del programa de firma se aplican al procedimiento del invento.

65

El código CS generado por el órgano signatario se envía al órgano verificador conjuntamente con la firma digital. Por ejemplo, se concatena en el momento de la firma. Como variante, se puede integrar directamente el código CS en la firma electrónica.

El órgano verificador recibe el código CS y la firma electrónica después de haber recibido previamente el mensaje electrónico. En el caso del algoritmo DSA, el órgano verificador va a calcular entonces el valor  $v$  con ayuda de la

clave pública y verificar que  $v$  es igual a  $r$ . Según una característica importante del invento, también debe verificar una segunda condición que pone la mira en asegurarse de que la firma fue generada por medios habilitados por el órgano verificador. Esta segunda condición constituye una seguridad suplementaria para el signatario y para el verificador. Si se verifican las dos condiciones, la firma será aceptada.

La segunda condición consiste en verificar que el código CS generado por el órgano signatario es aquel esperado por el órgano verificador.

Para realizar esta verificación, se genera en el órgano verificador, mediante un programa idéntico al del órgano signatario, una firma no personalizada establecida tomando como base un dato cualesquiera que reemplaza el dato secreto, ya que el órgano verificador no conoce el dato secreto. Un código CS' se genera a partir de instrucciones del programa que genera la firma no personalizada al igual que en el órgano signatario. Las instrucciones retenidas para generar el código CS' se seleccionan según los mismos criterios que en el órgano signatario. Al final, las instrucciones seleccionadas por el órgano verificador deben ser las mismas que aquellas seleccionadas por el órgano signatario. El código máquina de las instrucciones seleccionadas se somete entonces al mismo tratamiento lógico (operación O EXCLUSIVO o función de troceado) que aquel aplicado en el órgano signatario para generar el código CS. El código CS' así generado se compara seguidamente con el código CS. Si los códigos CS y CS' son diferentes, significa que la operación de generación de la firma no se ha desarrollado correctamente en el órgano que emitió la firma (es decir que no se desarrolló como previsto en el órgano verificador) y que la firma fue rechazada, aunque hubiera confirmado su autenticidad el órgano verificador. En cambio, si se cumplen las dos condiciones ( $v = r$  y  $CS' = CS$ ), se acepta la firma.

La figura 1 muestra el organigrama del procedimiento del invento en el caso de una generación y de una verificación de firmas electrónicas según un algoritmo DSA correspondiente al que se expone en el preámbulo de la presente solicitud.

El órgano signatario dispone de los parámetros  $p$ ,  $q$  y  $g$ , de la clave secreta  $x$ , de una función de troceado  $F$  y del mensaje  $m$ . En primer lugar, calcula la firma  $\{r, s\}$  y después el código CS por aplicación de la función de troceado  $F$  en la cadena de bits formada por ciertas instrucciones del programa de firma. La firma  $\{r, s\}$  y el código CS se transmiten al órgano verificador. El órgano verificador que conoce los parámetros  $p$ ,  $q$  y  $g$ , la clave pública  $y$ , la función de troceado  $F$  y el mensaje  $m$  calcula entonces  $v$  y verifica si  $v$  es igual a  $r$ . Según el invento, genera igualmente una nueva firma  $\{r, s\}$  tomando como base un dato cualesquiera  $x'$  de la misma longitud que la clave secreta  $x$  con ayuda de un programa de firma idéntico al del órgano signatario. Este programa se aplica en la máquina física o virtual del órgano signatario. Seguidamente, se genera un código CS' tomando como base las instrucciones del programa de firma que cumple con los mismos criterios que aquellos utilizados en el órgano signatario. Seguidamente se verifica que  $CS' = CS$ . Si las dos condiciones, a saber  $v = r$  y  $CS' = CS$ , no se han verificado, la firma  $\{r, s\}$  es rechazada por el órgano verificador.

El invento se aplica a todo tipo de sistema electrónico en el que un órgano signatario envía una firma electrónica a un órgano verificador encargado de verificar la validez de la firma. El órgano signatario puede ser por ejemplo una tarjeta inteligente de microprocesador y el órgano verificador un terminal de lectura de la tarjeta.

## REIVINDICACIONES

- 5 1. Procedimiento de firma electrónico, que comprende la generación de una firma digital por un órgano signatario que calcula esta firma en función de un dato secreto, y la verificación de la firma por un órgano verificador que verifica si dicha firma cumple una condición matemática, **caracterizado** porque el órgano signatario calcula además, durante la generación de la firma, un código representativo del programa empleado para generar dicha firma, y después lo transmite a dicho órgano verificador, dicho código generado es independiente del dato secreto, y porque la verificación consiste además en comprobar si la firma fue generada mediante un programa habilitado.
- 10 2. Procedimiento según la reivindicación 1, **caracterizado** porque la verificación de dicha segunda condición consiste en generar en el órgano verificador, mediante un programa idéntico al del órgano signatario, una firma no personalizada establecida tomando como base un dato cualesquiera que reemplaza dicho dato secreto con el fin de obtener el código representativo del programa empleado, y en compararlo con el código transmitido por el órgano signatario. La segunda condición se verifica si el código así generado por el órgano verificador y el código transmitido por el órgano signatario son idénticos.
- 15 3. Procedimiento según la reivindicación 2, **caracterizado** porque dicho código representativo del programa empleado para generar la firma se genera en el órgano signatario y en el órgano verificador tomando como base las instrucciones ejecutadas por el programa de generación de la firma, dichas instrucciones son independientes de dicho dato secreto y de dicho dato cualesquiera.
- 20 4. Procedimiento según la reivindicación 3, **caracterizado** porque, para generar el código representativo del programa, se seleccionan instrucciones del programa de generación de la firma, las cuales son independientes del dato secreto y del dato cualesquiera, y se combinan los códigos de las instrucciones seleccionadas entre sí por una operación de tipo O EXCLUSIVO.
- 25 5. Procedimiento según la reivindicación 3, **caracterizado** porque, para generar el código representativo del programa, se seleccionan instrucciones del programa de generación de la firma, las cuales son independientes de aquellas del dato secreto y de cualquier otro dato, y se realiza una operación de troceado en los códigos de las instrucciones seleccionadas.
- 30 6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado** porque el código representativo del programa generado por el órgano signatario se concatena en el momento de la firma y se transmite simultáneamente con ella.
- 35 7. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado** porque el código representativo del programa está integrado en la firma electrónica.
- 40 8. Ordenador que comprende un programa en condiciones de aplicar la generación del código representativo de un programa de firma según una de las reivindicaciones 1 a 7 en calidad de órgano signatario, ya sea en calidad de órgano verificador.
- 45 9. Ordenador según la reivindicación 8 **caracterizado** porque es un chip de microprocesador de un soporte de registro de tipo tarjeta inteligente.
- 50 10. Ordenador según la reivindicación 8 **caracterizado** porque es un lector de tarjeta inteligente.

50

55

60

65

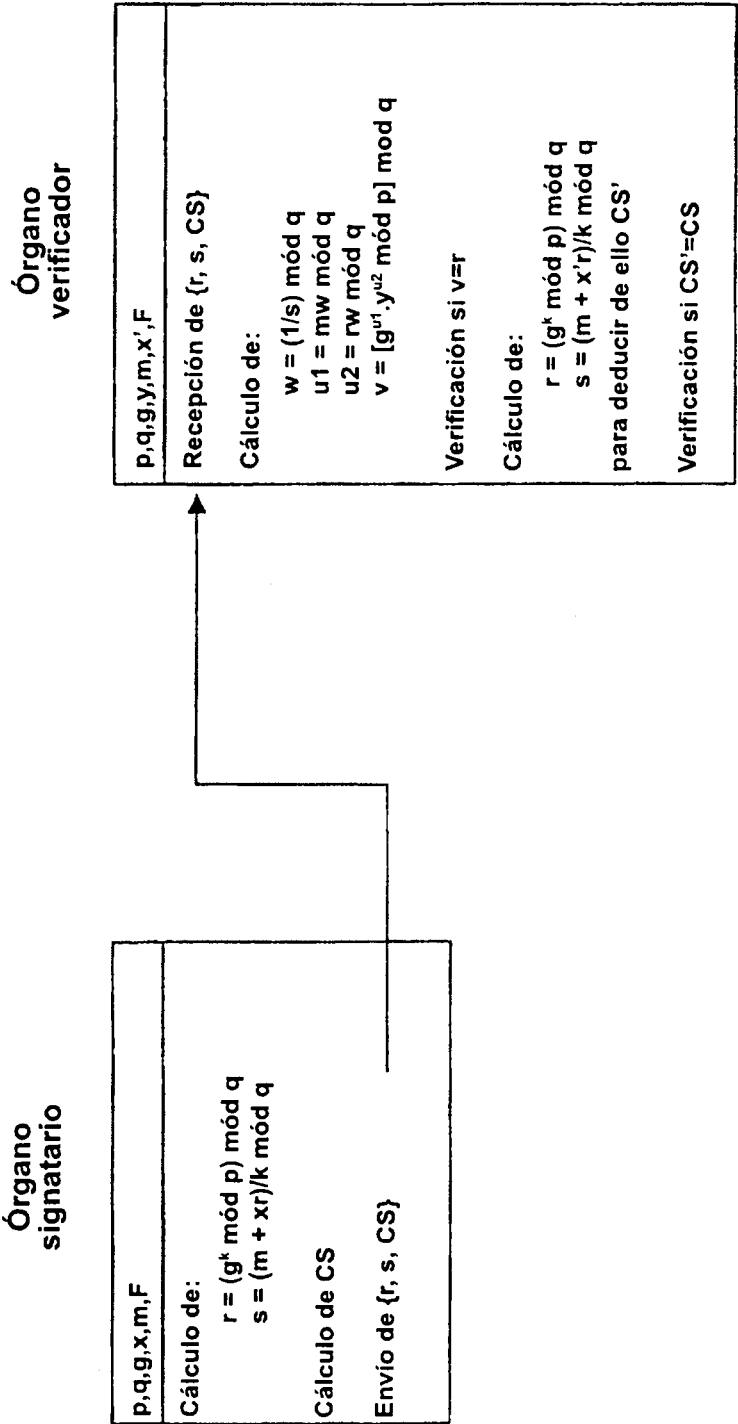


FIG.1