(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 367 725**

(51) Int. Cl.:
G06Q 20/00 (2006.01)
G07F 17/42 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08779067 .1**
(96) Fecha de presentación : **30.07.2008**
(97) Número de publicación de la solicitud: **2183713**
(97) Fecha de publicación de la solicitud: **12.05.2010**

(54) Título: **Emisión de bonos electrónicos.**

(30) Prioridad: **31.07.2007 EP 07113541**

(45) Fecha de publicación de la mención BOPI:
08.11.2011

(45) Fecha de la publicación del folleto de la patente:
08.11.2011

(73) Titular/es: **NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO**
Schoemakerstraat 97
2628 VK Delft, NL

(72) Inventor/es: **Veugen, Thijs y**
Danes, Luuk

(74) Agente: **Durán Moya, Carlos**

DESCRIPCIÓN

Emisión de bonos electrónicos

La presente invención se refiere a la emisión de bonos electrónicos. Más en particular, la presente invención se refiere a un método y a un dispositivo para producir y/o emitir bonos electrónicos que se pueden entregar a un comerciante a cambio de bienes y/o servicios.

Se conoce la emisión de bonos electrónicos que se puedan intercambiar por bienes y servicios. La solicitud de patente europea EP 0 823 694 (KPN) da a conocer "tiques" o bonos electrónicos que se pueden almacenar en una tarjeta inteligente, mientras que la solicitud de patente internacional WO 00/30045 (KPN) da a conocer bonos electrónicos que también se pueden imprimir. Los bonos de la solicitud WO 00/30045 contienen datos de identificación para identificar el servicio a prestar.

Estos bonos electrónicos se pueden adquirir utilizando dinero corriente y posteriormente se pueden almacenar en una tarjeta inteligente que el usuario lleva en su monedero. La tarjeta inteligente se utiliza en un punto de venta para presentar el bono a cambio de bienes o servicios. En lugar de los bonos electrónicos a veces se utilizan las monedas electrónicas.

Un problema que puede ocurrir con los bonos electrónicos o el dinero electrónico es su uso fraudulento: un usuario puede ser capaz de gastar el mismo bono o moneda dos veces. Los bonos electrónicos de la solicitud WO 00/30045 se "sellan" cuando se utilizan a efectos de evitar que se utilicen más de una vez. No obstante, los usuarios fraudulentos pueden encontrar maneras de evitar o incluso deshacer dicho "sello" y utilizar el mismo bono de nuevo. En consecuencia, un usuario fraudulento puede cometer fraude repetidamente.

La patente de Estados Unidos US 4 987 593 (Chaum) da a conocer un sistema de dinero electrónico que utiliza firmas digitales. Se puede recuperar cierta información contenida en el dinero electrónico bajo ciertas condiciones, permitiendo identificar, de esta manera, a los usuarios fraudulentos del sistema. No obstante, el fraude sólo puede detectarse cuando un usuario gasta un artículo de dinero electrónico más de una vez ("gasto doble"). Esto no evita que un usuario fraudulento reciba nuevo dinero electrónico, ni existe garantía de que el usuario utilice los bienes o servicios con el dinero de una manera honesta y legal. En consecuencia, este sistema conocido puede identificar a los usuarios que gastan el doble pero aún emiten nuevo dinero electrónico en caso de fraude.

Es un objetivo de la presente invención superar estos y otros problemas de la técnica anterior y proporcionar un método y un dispositivo para emitir bonos electrónicos que un usuario puede presentar a un comerciante a cambio de bienes o servicios, cuyo método y dispositivo tienen una resistencia mejorada al fraude.

Es otro objetivo de la presente invención proporcionar un método y un dispositivo para emitir bonos electrónicos que evite que los usuarios fraudulentos comentan fraude repetidamente.

En consecuencia, la presente invención proporciona un método de emisión de bonos electrónicos que un usuario puede presentar a un comerciante a cambio de bienes o servicios, comprendiendo dicho método las etapas de:

- un emisor recibe una declaración electrónica del usuario,
- el emisor verifica si la declaración electrónica incluye una firma de un comerciante en un bono electrónico anterior, y
- el emisor proporciona una firma en un nuevo bono electrónico únicamente si la declaración electrónica incluye dicha firma.

Al firmar solamente un nuevo bono electrónico y, de esta manera emitiendo un nuevo bono electrónico válido, si una declaración electrónica recibida del usuario contiene una firma de un comerciante, se asegura que únicamente los usuarios de buena fe reciben nuevos bonos. Cada vez que un usuario (por ejemplo, un consumidor) utiliza un bono para obtener bienes y/o servicios y, por tanto, entrega su bono a cambio de bienes y/o servicios, el comerciante que provee dichos bienes y/o servicios puede firmar el bono si se comprueba que es válido. Esta firma realizada por un comerciante en un bono válido utilizado es una prueba de que el usuario no era fraudulento. Presentando este bono utilizado firmado al emisor se puede obtener un nuevo bono electrónico. Sin esta declaración, el emisor no emitirá un nuevo bono electrónico a este usuario.

Los expertos en la técnica reconocerán que una firma sobre un bono electrónico es una firma electrónica que implica técnicas criptográficas, tal como se explicará más adelante en más detalle.

Cada uno de los bonos tiene preferentemente una identificación única (por ejemplo, un número de serie) lo que permite distinguirlo de otros bonos a efectos de comprobar que se utilizan sólo una vez. La característica inventiva de solicitar una declaración válida (es decir, firmada) evita que un usuario fraudulento reciba nuevos bonos. En el método de la presente invención, el emisor verifica si la declaración electrónica incluye una firma de un comerciante en un bono electrónico anterior. Dado que el primer bono electrónico no tendrá ningún bono electrónico anterior y,

por tanto, ninguna declaración, se prefiere que el emisor proporcione una firma en un primer bono electrónico para el usuario en ausencia de una declaración. Esto asegura que el usuario pueda recibir un primer bono electrónico. Cualesquiera bonos electrónicos posteriores se emitirán típicamente sólo cuando se pueda presentar una declaración válida. Además, se prefiere que cada usuario pueda recibir un primer bono electrónico firmado en la ausencia de una declaración. No obstante, se pueden prever realizaciones en las que únicamente un número limitado de usuarios reciban un primer bono electrónico firmado sin haber presentado una declaración electrónica válidamente firmada, estando limitado posiblemente este número limitado de usuarios a un único usuario.

Los bonos electrónicos pueden ser generados por el emisor. No obstante, esto limitaría la privacidad del usuario, dado que el emisor tendría toda la información en relación al bono. Por tanto, en una realización preferente de la presente invención la etapa de recibir una declaración electrónica incluye, además, la recepción del nuevo bono electrónico por parte del usuario para ser firmado. Es decir, los bonos electrónicos no son generados por el emisor sino por el usuario o terceros y se transfieren al emisor, preferentemente conjuntamente con una declaración electrónica.

Los bonos electrónicos pueden contener información que identifica al usuario o al comerciante donde se va a gastar el bono. A efectos de no revelar esta información al emisor, el usuario puede bloquear ventajosamente el bono electrónico antes de que el emisor lo reciba. Este bloqueo lo puede realizar el usuario multiplicando el bono electrónico por un factor de bloqueo elevado a una potencia igual a una clave pública del emisor (módulo N), cuyo primer factor de bloqueo es preferentemente igual a un número aleatorio elevado a una potencia igual a una clave pública del comerciante (módulo N), donde N es un entero largo igual a un producto de números primos. Tal como se hará evidente más adelante a partir de la descripción detallada de la invención, al multiplicar el bono electrónico por dicho primer factor de bloqueo elevado a la potencia igual a una clave pública del emisor, proporciona un esquema de bloqueo muy efectivo y eficiente.

En lugar de bloquear el bono electrónico, o además de bloquearlo, el usuario puede bloquear también la declaración electrónica antes de que el emisor la reciba, para evitar que el emisor obtenga información en relación a los bienes o servicios adquiridos anteriormente. Más en particular, el usuario puede multiplicar ventajosamente la declaración electrónica por un segundo factor de bloqueo elevado a una potencia igual a una clave pública del emisor (módulo N), cuyo segundo factor de bloqueo es preferentemente un número aleatorio.

El método de la presente invención permite generar, emitir y gastar bonos electrónicos de manera anónima a la vez que asegura que los usuarios fraudulentos no recibirán ningún bono electrónico nuevo. En una realización preferente, es posible además determinar la identidad de un usuario fraudulento que utiliza el mismo bono más de una vez. Para este fin, el bono electrónico puede contener la identidad del usuario oculta, cuya identidad puede ser revelada si el bono electrónico se presenta a un comerciante más de una vez. Más en particular, el bono electrónico puede obtenerse, en esta realización, sumando la identidad del usuario a un número aleatorio para obtener un valor de suma, utilizando el valor de suma y una primera función unidireccional para generar un primer valor intermedio, utilizando el número aleatorio y la primera función unidireccional para generar un segundo valor intermedio y utilizando el primer y segundo valores intermedios y una segunda función unidireccional para generar el bono electrónico.

Un bono electrónico obtenido de esta manera contiene la identidad del usuario, pero las funciones unidireccionales y el número aleatorio evita que esta identidad se determine bajo circunstancias normales. No obstante, si se requiere que el usuario entregue o bien el valor de suma y el segundo valor intermedio o bien el número aleatorio y el primer valor intermedio, cada vez que se ofrece un bono electrónico a un comerciante, generalmente será posible que el comerciante determine la identidad a partir del valor de suma y del valor aleatorio si el bono electrónico es ofrecido más de una vez.

Las firmas de los bonos electrónicos y de las declaraciones se pueden obtener de diversas maneras. No obstante, se prefiere obtener una firma elevando un valor a firmar a una potencia, donde la potencia es la inversa (módulo de una función de N, donde N es un entero predeterminado) de una clave pública de la entidad firmante.

En la presente invención se prefiere que un bono electrónico firmado incluya un bono electrónico sin firmar así como la firma del emisor en el bono electrónico sin firmar.

La presente invención también da a conocer un método de utilización de un bono electrónico generado por el método definido anteriormente, comprendiendo dicho método las etapas de:

- el usuario entrega el bono electrónico a un comerciante,
- el comerciante verifica si el bono electrónico incluye la firma del emisor, y
- el comerciante únicamente proporciona bienes o servicios si el bono electrónico incluye dicha firma del emisor.

En una realización preferente, la etapa de entrega del bono electrónico comprende además la entrega bien de un primer valor intermedio y de un número aleatorio o de un segundo valor intermedio y de un valor de suma relacionados con una identificación del usuario, a efectos de poder determinar la identificación del usuario cuando el

mismo bono se recibe más de una vez.

La presente invención proporciona, además, un producto de programa de ordenador para llevar a cabo el método, tal como se ha definido anteriormente. Un producto de programa de ordenador puede comprender un conjunto de instrucciones ejecutables en ordenador almacenadas en un portador de datos, tal como un CD o un DVD. El conjunto de instrucciones ejecutables en ordenador, que permite a un ordenador programable llevar a cabo el método, tal como se ha definido anteriormente, también puede descargarse desde un servidor remoto, por ejemplo a través de internet.

La presente invención también da a conocer un dispositivo para emitir bonos electrónicos que un usuario puede entregar a un comerciante a cambio de bienes o servicios, comprendiendo el dispositivo:

- una unidad receptora para recibir una declaración electrónica del usuario,
- una unidad de verificación para verificar si la declaración electrónica incluye una firma del comerciante en un bono electrónico anterior, y
- una unidad de emisión para proporcionar una firma en un nuevo bono electrónico únicamente si la declaración electrónica incluye dicha firma del comerciante.

El dispositivo tiene las mismas ventajas que el método tratado anteriormente.

La presente invención proporciona, además, un sistema para proporcionar bienes y/o servicios a cambio de bonos, comprendiendo el sistema un dispositivo emisor, tal como se ha descrito anteriormente. El sistema comprende, además, preferentemente, al menos un dispositivo de usuario y al menos un dispositivo de comerciante para utilizar en el método definido anteriormente.

La presente invención se explicará en más detalle a continuación con referencia a las realizaciones de ejemplo mostradas en los dibujos adjuntos, en los que:

la figura 1 muestra de manera esquemática el intercambio de datos entre un usuario, un comerciante y un emisor de acuerdo con la presente invención.
La figura 2 muestra de manera esquemática un dispositivo para emitir bonos de acuerdo con la presente invención.

El intercambio de datos entre un usuario U, un emisor I y un comerciante M se representa esquemáticamente en la figura 1. El usuario U puede ser una persona que porta una tarjeta inteligente, un monedero electrónico o un dispositivo similar. En el caso de transacciones por internet, el usuario puede ser una persona que tiene un ordenador o dispositivo similar a su disposición. El comerciante M puede ser una tienda que tiene una caja registradora dispuesta para pagos electrónicos, o un teatro, instalación deportiva, estación de autobuses u otra entidad que proporcione bienes y/o servicios a cambio de bonos electrónicos y estén equipados de manera similar. En el caso de transacciones por internet, puede que no haya ningún dispositivo para transacciones electrónicas presente en la misma tienda o teatro, teniendo lugar las transacciones electrónicas en un servidor remoto. El emisor I puede ser un banco, oficina postal, oficina municipal u otra entidad dispuesta para emitir bonos electrónicos.

En el método de la presente invención, la “emisión” de bonos electrónicos V_i implica la firma de bonos sin firmar V_i^*, es decir, aplicar una firma electrónica S_I del emisor I a un bono electrónico sin firmar V_i^*, y posteriormente combinar la firma electrónica formada de esta manera con el bono sin firmar V_i^*:

$$V_i = \{S_I(V_i^*), V_i^*\} \qquad (1)$$

En otras palabras, un bono firmado V_i es una combinación de un bono sin firmar V_i^* y de la firma del emisor $S_I(V_i^*)$ en dicho bono sin firmar V_i^*. Dicha combinación comprende preferentemente una concatenación. Los bonos electrónicos sin firmar V_i^* son proporcionados por el usuario U, en el ejemplo mostrado.

El comerciante M acepta los bonos electrónicos firmados V_i que tienen el formato de la fórmula (1) y, de esta manera, comprenden sus equivalentes sin firmar V_i^*. Se comprueba la firma de cada bono electrónico V_i recibido por el comerciante M. Los bonos sin firmar V_i^* no acompañados por una firma $S_I(V_i^*)$ o acompañados por una firma incorrecta son rechazados.

De acuerdo con la presente invención, el emisor I únicamente genera un nuevo bono electrónico firmado V_i si el emisor I ha recibido una declaración D_{i-1}. Dicha declaración D_{i-1} es generada por el comerciante M y se entrega al usuario U únicamente si el usuario se ha comportado correctamente, es decir, si el bono electrónico anterior V_{i-1} era válido y se utilizó una sola vez. Esta declaración D_{i-1} es preferentemente una versión firmada del bono electrónico anterior (sin firmar) V_{i-1}^*:

$$D_{i-1} = S_M(V_{i-1}^*) \qquad (2),$$

donde S_M es una firma electrónica del comerciante M. En otras palabras, el comerciante firma y devuelve el bono

gastado al usuario si, y sólo si, el usuario resultó ser de buena fe. En consecuencia, el usuario sólo recibe un bono firmado nuevo V_i del emisor si el bono V_{i-1}^* anterior fue firmado por el comerciante. De esta manera, se evita que los usuarios fraudulentos reciban nuevos bonos.

Los bonos electrónicos V_i utilizados en la presente invención son representados por números enteros o comprenden los mismos. Estos números son determinados preferentemente por el usuario o su monedero electrónico o tarjeta inteligente. En una realización preferente, un bono electrónico V_i^* (sin firmar) tiene el siguiente formato:

$$V_i^* = G(F(a_i), F(a_i+Q)) \qquad (3),$$

donde a_i es un número aleatorio, Q es la identidad del usuario, y F y G son funciones unidireccionales. Como es bien sabido por los expertos en la técnica, es fácil calcular el valor de una función unidireccional (por ejemplo, F) dada una variable de entrada (por ejemplo, a_i), pero es prácticamente imposible determinar la inversa de la función, es decir, calcular el valor de la variable de entrada dado el valor de la función unidireccional.

El número aleatorio a_i puede ser generado por el dispositivo del usuario (por ejemplo, una tarjeta inteligente), mientras que la identidad Q puede ser un número de identidad asociado con el dispositivo del usuario. Un bono electrónico que se determina utilizando la fórmula anterior (3) es, por tanto, un número que depende de la identidad del usuario. No obstante, las funciones unidireccionales F y G evitan que esta identidad sea determinada por el comerciante o por el emisor. Únicamente si se proporciona información adicional se puede derivar la identidad Q del bono (o del valor del mismo). La función unidireccional G incluso evita que los valores intermedios $F(a_i)$ y $F(a_i+Q)$ sean determinados a partir del valor del bono V_i^*.

De acuerdo con un aspecto adicional de la presente invención, la identidad Q del usuario puede ser revelada si el usuario intenta entregar el mismo bono más de una vez. Esto se puede conseguir si se requiere que el usuario entregue bien el valor intermedio $F(a_i)$ y el valor de suma (a_i+Q) o el valor aleatorio a_i y el valor intermedio $F(a_i+Q)$ al comerciante cuando se entrega un bono. Cuando se entrega el mismo bono que contiene el mismo número aleatorio a_i dos veces, es muy probable (e incluso cierto en realizaciones en línea) que el comerciante habrá obtenido tanto a_i como (a_i+Q), permitiendo que se determine la identidad Q.

Se entenderá que la elección del par de valores a entregar al comerciante es determinada por el comerciante, no por el usuario. El comerciante (dispositivo) puede compilar una lista de usuarios que entregaron bonos, utilizando la lista para determinar qué par de valores se debe entregar. En realizaciones en línea, dicha lista puede ser almacenada centralmente, por ejemplo en el emisor. De manera alternativa, el comerciante puede solicitar de manera aleatoria un par de valores.

La entrega bien del valor intermedio $F(a_i)$ y del valor de suma (a_i+Q) o del valor aleatorio a_i y del valor intermedio $F(a_i+Q)$ al comerciante sirve para otro propósito: utilizando las funciones F y G, el comerciante puede comprobar si el bono V_i^* es correcto, es decir, si se cumple $V_i^* = G(F(a_i), F(a_i+Q))$.

Las firmas S_I y S_M utilizadas en la presente invención implican preferentemente elevar un número (tal como el número que representa un bono electrónico) a una potencia igual a la inversa de una clave pública:

$$S_I(V_i^*) = (V_i^*)^{1/KI} \qquad (4),$$

donde KI es la clave pública del emisor I. De manera similar, la firma del comerciante se puede escribir como:

$$S_M(V_{i-1}^*) = (V_{i-1}^*)^{1/KM} \qquad (5),$$

donde KM es la clave pública del comerciante M.

Como es habitual en los cálculos criptográficos, los números se calculan módulo N. Esto hace extremadamente difícil determinar la inversa. Como resultado, la inversa de una clave pública es conocida únicamente por una sola parte, aún si todas las partes conocen la clave pública.

En consecuencia, el comerciante M puede verificar la firma del emisor I elevando el bono firmado V_i a una potencia igual a la clave pública del emisor KI: $S_I(V_i^*)^{KI} = ((V_i^*)^{1/KI})^{KI} = V_i^*$, si la firma S_i era correcta. De manera similar, el emisor I puede verificar si la declaración D_{i-1} es igual al bono anterior firmado por el comerciante M (de hecho, firmado tanto por el comerciante M como por el emisor I) elevando la declaración D_i a una potencia (módulo N) igual a la clave pública del comerciante M: $(D_{i-1})^{KM} = ((V_{i-1}^*)^{1/KM})^{KM} = V_{i-1}^*$, si la firma S_M era correcta. Este mecanismo de verificación hace uso del hecho de que una clave pública está disponible, pero calcular la inversa de una clave pública, módulo N, no es factible, tal como se ha mencionado anteriormente.

La descripción anterior explica una realización básica de la presente invención. En las realizaciones preferentes, los factores de bloqueo se utilizan para proteger el anonimato del usuario, y también proporcionan un mecanismo de verificación adicional. Estas características adicionales se utilizan preferentemente en conjunto, pero se puede omitir cualquiera de ellas de una realización sin desviarse de la presente invención.

Una realización preferente de la presente invención comprende las siguientes etapas. Se supondrá que el usuario ha recibido una declaración del comerciante tras gastar un bono anterior y que el usuario y/o el emisor han determinado un identificador de usuario Q que es conocido por ambos.

El dispositivo de usuario genera primero una serie de números aleatorios a_i y s_i, con i = 1, ..., M (pueden existir valores diferentes de M para a_i y s_i). Se utiliza un número s_i para generar un (primer) factor de bloqueo r_i elevando s_i a una potencia igual a KM (módulo N), donde KM es la clave pública del comerciante M donde el usuario pretende gastar el bono:

$$r_i = s_i^{KM} \qquad (6).$$

Utilizando el número aleatorio a_i y la identificación del usuario Q, el dispositivo de usuario también genera bonos (sin firmar) V_i^* de acuerdo con la fórmula (3) anterior:

$$V_i^* = G(F(a_i), F(a_i+Q)) \qquad (3'),$$

donde F y G son funciones unidireccionales. El usuario (dispositivo) genera entonces números x_i que se entregan al emisor I, donde:

$$x_i = r_i^{KI} \cdot V_i^* \qquad (7),$$

donde '.' indica multiplicación (módulo N) y KI es la clave pública del emisor I, como antes.

En una realización particularmente preferente, el usuario entrega k números x_i al emisor I, donde k es un entero mayor que 1. En consecuencia, el emisor recibe los números x_i, ..., x_k y solicita que el usuario "abra" (k-1) de esos números. Es decir, se solicita que el usuario dé a conocer el valor a_i y s_i de esos (k-1) números x_i, permitiendo de esta manera que el emisor verifique si los bonos V_i^* son correctos.

Si estos bonos son correctos, el emisor firma el número x_i restante y el usuario recibe el número $S_I(x_i)$.As $x_i = r_i^{KI}.V_i^*$ y $S_I(x_i) = x_i^{1/KI}$ firmado, el número $S_I(x_i)$ firmado es igual a $x_i^{1/KI} = (r_i^{KI}.V_i^*)^{1/KH} = r_i.(V_i^*)^{1/KI} = r_i.(V_i^*)$. El emisor registra la emisión de un bono, por ejemplo registrando el número que representa el valor V_i y cualquier número de serie del bono.

Posteriormente el usuario sólo necesita dividir el número firmado $S_I(x_i)$ por r_i para obtener el bono V_i firmado. El usuario también puede comprobar la firma elevando $S_I(x_i)$ a una potencia igual a la clave pública KI, obteniendo de esta manera x_i si la firma S_I es correcta.

El bono V_i puede ahora ser gastado en el comerciante M. Para este fin, el usuario entrega el bono V_i firmado (que comprende el bono V_i^* sin firmar correspondiente) al comerciante M, que comprueba la firma del emisor elevando la firma $S_I(V_i^*)$ a una potencia igual a la clave pública KI del emisor y comparando el resultado con el bono V_i^* sin firmar, como antes. El bono V_i firmado es almacenado preferentemente por el comerciante para su comparación con futuros bonos.

Posteriormente, el comerciante pide al usuario que "abra" el bono V_i^* (sin firmar) entregando bien $F(a_i)$ y (a_i+Q) o a_i y $F(a_i+Q)$, ver fórmula (3). El comerciante almacena estos valores y los utiliza para comprobar el bono V_i^*. El comerciante puede comprobar también si un bono que tenga el mismo valor se ha entregado antes comparando el bono con los bonos entregados anteriormente.

Si se encuentra que el bono es válido y es entregado por primera vez, se proporcionarán los bienes y/o servicios para los que se ha gastado el bono. Además, si el bono se entrega por primera vez, el comerciante M proporciona una declaración D_i igual al bono V_i^* gastado firmado por el comerciante: $D_i = S_M(V_i^*) = (V_i^*)^{1/KM}$, donde KM es la clave pública del comerciante.

En las realizaciones preferentes de la presente invención, en lugar de entregar la declaración D_i al emisor, el usuario entrega una declaración (bloqueada) d_i utilizando un (segundo) factor de bloqueo igual a un número s_i elevado a una potencia igual a la clave pública del emisor KI:

$$d_i = s_i^{KI} \cdot D_i = s_i^{KI} \cdot S_M(V_i^*) \qquad (8),$$

donde s_i es el número aleatorio correspondiente al bono V_i, como antes. Este factor de bloqueo s_i^{KI} oculta la información que identifica los bienes y/o servicios adquiridos por el usuario. Aún, el emisor puede verificar que $d_i = S_M(x_i)$, siendo x_i el número que el emisor recibió antes:

$$S_M(x_i) = S_M(r_i^{KI} \cdot V_i^*) = S_M((s_i^{KM})^{KI} \cdot V_i^*) = S_M(s_i^{KM \cdot KI}) \cdot S_M(V_i^*) = s_i^{KI} \cdot S_M(V_i^*) = d_i.$$

Si esta verificación es satisfactoria, el emisor registrará que el bono V_i asociado a x_i ha sido gastado y disminuirá en uno el contador para bonos pendientes.

Son posibles diversas modificaciones. El emisor puede utilizar diferentes firmas electrónicas para diferentes tipos de bienes y/o servicios, o puede utilizar una única firma electrónica para todos los tipos de bienes y servicios. Los bonos pueden contener más información, por ejemplo una fecha o el número de personas para las que el bono es válido. En general, un bono sin firmar se puede escribir así:

$$V_i^* = G(F(a_i), F(a_i+Q), X) \qquad (3a),$$

donde X es información adicional que puede incluir una fecha. En otra realización un bono (sin firmar) puede escribirse así:

$$V_i^* = G(F(a_i)) \,.\, G(F(a_i+Q)) \qquad (3b),$$

o

$$V_i^* = G(F(a_i)) \,.\, G(F(a_i+Q)) \,.\, G(X) \qquad (3c),$$

en otras palabras, un producto de funciones unidireccionales. Si no es necesario determinar la identidad de un usuario fraudulento por medio de un bono, la identidad Q puede ser omitida del bono, dando como resultado:

$$V_i^* = G(F(a_i)) \qquad (3d),$$

o incluso

$$V_i^* = F(a_i) \qquad (3e).$$

Se puede incorporar un número de serie o información confidencial en la información adicional X, pero también se puede incorporar como información concatenada Y:

$$V_i^* = G(F(a_i), F(a_i+Y|Q)) \qquad (3f),$$

donde "|" indica concatenación.

En lugar de "abrir" (k-1) bonos al emisor, tal como se ha descrito anteriormente, se podría "abrir" un número (k-m) menor de bonos, donde m es mayor que uno.

Los ejemplos tratados anteriormente implican un único comerciante M que tiene una única clave pública M. Si el método o sistema de la presente invención implica múltiples comerciantes, todos pueden utilizar la misma clave pública. Esto tiene la clara ventaja de la simplicidad. No obstante, se puede obtener un método y sistema más seguros si se utiliza un producto de claves públicas de comerciante, en lugar de una única clave pública de comerciante.

El método, dispositivo y sistema de la presente invención se puede adaptar para sistemas de seudónimos. En un sistema de seudónimos, el usuario U y el emisor I pueden generar conjuntamente un seudónimo

$$P_{UI} = a_I^{xU} \,.\, b_I^{sUI} \qquad (9)$$

donde los números a_i y b_I son proporcionados por el emisor I (y donde el número a_i no está relacionado con los números a_i mencionados anteriormente), y donde únicamente el usuario U conoce los coeficientes (es decir, exponentes) x_U y s_{UI}. Por tanto, el emisor conoce el seudónimo P_{UI} resultante sin conocer x_U y s_{UI}.

El método de la invención tal como se ha descrito anteriormente se modifica adicionalmente de manera que el usuario U genera primero bonos electrónicos V_i^* (sin firmar) de acuerdo con la fórmula (3) anterior, pero posteriormente modifica estos bonos V_i^* para generar bonos electrónicos W_i^* (sin firmar) modificados de acuerdo con:

$$W_i^* = g_U^{Vi^*} \,.\, h_U^{ri} \qquad (10),$$

donde los coeficientes g_U y h_U son únicamente conocidos por el usuario U, y donde r_i es un número aleatorio generado por el usuario U.

Posteriormente, el usuario U presenta estos bonos electrónicos W_i^* modificados, en lugar de los bonos V_i^*, al emisor I. En respuesta, el emisor pedirá al usuario que "abra", por ejemplo, (k-1) bonos W_i^* presentando los valores correspondientes de r_i y a_i, similar al método descrito anteriormente, de manera que el emisor I puede verificar estos bonos. El emisor I firma posteriormente el bono electrónico W_i^* restante y ofrece la firma (c_I, e_I) al usuario, donde

$$c_I^{eI} = P_{UI} \,.\, d_I \,.\, W_i^* \qquad (11),$$

y donde d_I es un valor conocido por todas las partes.

Cuando se utiliza un bono electrónico, el usuario U ofrece un bono electrónico (sin firmar) V_i^* (en lugar del bono V_i

firmado) al comerciante M. Posteriormente, se lleva a cabo una prueba de protocolo de conocimientos en la que el usuario U prueba conocer los valores:

$$x_U, s_{UI}, c_I, e_I, r_i$$

de manera que

$$c_I^{eI} = a_I^{xU} \cdot b_I^{sUI} \cdot d_I \cdot g_I^{Vi*} \cdot h_I^{ri} \qquad (12),$$

donde el comerciante M conoce los números a_I, b_I, d_I, g_I y h_I y puede determinar g_I^{Vi*}.

Posteriormente, el comerciante M solicita que el usuario U muestre bien el primero o el segundo argumento de la función G, como antes.

La declaración D_i es en esta realización una firma digital del comerciante M en el tique V_i^*: la firma es (c_M, e_M), de manera que

$$c_M^{eM} = g_M^{Vi*} \qquad (13).$$

Cuando se entrega la declaración, el usuario U presenta su seudónimo P_{UI} y su bono W_i^* (bloqueado). Posteriormente, el usuario U y el emisor I realizan una prueba de protocolo de conocimientos en la que el usuario prueba que conoce los valores

$$c_M, e_M, V_i^*, r_i,$$

de manera que

$$c_M^{eM} = g_M^{Vi*} \text{ and } W_i^* = g_I^{Vi*} \cdot h_U^{ri} \quad (14)$$

donde el emisor I conoce los números g_M, W_i^*, g_I y h_I. Además, se tiene que demostrar que ambas instancias de V_i^* son iguales. De esta manera, la presente invención se puede utilizar en sistemas de seudónimos. Los expertos en la técnica se darán cuenta que se pueden utilizar otros seudónimos distintos de los dados por la fórmula (9).

Un mero ejemplo de la realización de un dispositivo de emisor I se muestra en más detalle en la figura 2. Dicho dispositivo de emisor I se puede utilizar en todas las realizaciones de la presente invención.

El dispositivo de emisor -10- mostrado de manera esquemática y únicamente por medio de un ejemplo no limitativo en la figura 2 comprende una unidad receptora (RU) -11-, una unidad de verificación (VU) -12- y una unidad de emisión (IU) -13-. La unidad receptora -11- se dispone para recibir un bono electrónico sin firmar V_i^* y una declaración electrónica D_i. La unidad de verificación -12- se dispone para verificar la declaración D_i o, en una realización preferente, la declaración bloqueada d_i. La unidad de emisión -13- se dispone para emitir un bono electrónico firmando el bono sin firmar V_i^*.

Un dispositivo de usuario (-U- en la figura 1), de acuerdo con la presente invención, puede estar compuesto por un monedero electrónico que comprende un microprocesador, una memoria que almacena programas de software adecuados y un circuito de entrada-salida para comunicarse con una tarjeta inteligente o un portador de bonos similar. Más en particular, el dispositivo de usuario, de acuerdo con la presente invención, puede generar bonos y factores de bloqueo y comprobar firmas.

Un dispositivo de comerciante (-M- en la figura 1), de acuerdo con la presente invención, puede estar formado por una caja registradora electrónica dispuesta para el pago electrónico y también puede comprender un microprocesador, una memoria que almacena programas de software adecuados y un circuito de entrada-salida para comunicarse con una tarjeta inteligente o portador de bonos similar. La tarjeta inteligente puede ser una tarjeta inteligente convencional dispuesta para almacenar bonos electrónicos.

Tal como se ha mencionado anteriormente, los bonos electrónicos utilizados en la presente invención se pueden almacenar en una memoria electrónica, por ejemplo, la memoria RAM (memoria de acceso aleatorio) de un dispositivo de usuario o de un dispositivo de comerciante. Más en particular, los bonos electrónicos y las declaraciones electrónicas se representan mediante números almacenados en la memoria electrónica y se procesan en circuitos electrónicos, por ejemplo, un procesador o un microprocesador. Los bonos tienen preferentemente una identificación única, tal como un número de serie. La firma de un comerciante en un bono gastado es prueba del comportamiento de buena fe del usuario. Aunque la invención se ha explicado con referencia a un único usuario, un único comerciante y un único emisor, se entenderá que la mayoría de realizaciones implicarán a múltiples usuarios, múltiples comerciantes y/o múltiples emisores. La invención se puede utilizar tanto en línea como fuera de línea.

La presente invención se basa en la idea de que el uso fraudulento de bonos electrónicos se puede reducir significativamente solicitando una declaración de un comerciante cuando se emiten nuevos bonos, cuya declaración se proporciona únicamente cuando el usuario no ha cometido ningún fraude. La presente invención se beneficia de la idea adicional de que el solicitar información de identificación parcial cuando se entrega un bono permite determinar la información de identificación completa cuando se entrega el mismo bono más de una vez.

REIVINDICACIONES

1. Método para generar bonos electrónicos firmados (V_i) que un usuario (U) puede entregar a un comerciante (M) a cambio de bienes o servicios, comprendiendo el método las etapas de:

un emisor (I) recibe una declaración electrónica (D_{i-1}) del usuario (U),

- el emisor verifica si la declaración electrónica (D_{i-1}) comprende una firma (S_M) de un comerciante (M) en un bono electrónico sin firmar (V_{i-1}^*) anterior del usuario y
- el emisor proporciona una firma (S_I) en un bono electrónico (V_i*) sin firmar, nuevo, del usuario únicamente si la declaración electrónica comprende dicha firma (S_M) del comerciante.

2. Método, según la reivindicación 1, en el que el emisor (I) proporciona una firma (S_I) en un primer bono electrónico (V_1^*) para el usuario (U) en la ausencia de una declaración (D_{i-1}).

3. Método, según la reivindicación 1 ó 2, en el que la etapa de recibir una declaración electrónica (D_{i-1}) incluye, además, la recepción del usuario (U) del nuevo bono electrónico (V_i^*) para firmar.

4. Método, según la reivindicación 3, en el que el usuario (U) bloquea el bono electrónico (V_i^*) antes de que el emisor (I) lo reciba.

5. Método, según la reivindicación 4, en el que el usuario (U) multiplica el bono electrónico (V_i^*) por un primer factor de bloqueo (r_i) elevado a una potencia igual a una clave pública (KI) del emisor (I), cuyo primer factor de bloqueo (r_i) es preferentemente igual a un número aleatorio (s_i) elevado a una potencia igual a una clave pública (KM) del comerciante (M).

6. Método, según cualquiera de las reivindicaciones precedentes, en el que el usuario (U) bloquea la declaración electrónica (D_{i-1}) antes de que la reciba el emisor (I).

7. Método, según la reivindicación 6, en el que el usuario (U) multiplica la declaración electrónica (D_{i-1}) por un segundo factor de bloqueo (s_i) elevado a una potencia igual a una clave pública (KI) del emisor (I), cuyo segundo factor de bloqueo (s_i) es preferentemente un número aleatorio.

8. Método, según cualquiera de las reivindicaciones precedentes, en el que el bono electrónico (V_i^*) contiene la identidad (Q) oculta del usuario (U).

9. Método, según la reivindicación 8, en el que el bono electrónico (V_i^*) se obtiene sumando la identidad (Q) del usuario (U) a un número aleatorio (a_i) para obtener un valor de suma (a_i+Q), utilizando el valor de suma y una primera función unidireccional (f) para generar un primer valor intermedio (f(a_i+Q)), utilizando el número aleatorio (a_i) y la primera función unidireccional (f) para generar un segundo valor intermedio (f(a_i)), y utilizando los valores intermedios primero y segundo y una segunda función unidireccional (g) para generar el bono electrónico (V_i^*).

10. Método, según cualquiera de las reivindicaciones precedentes, en el que una firma (S_I, S_M) se obtiene elevando un valor a firmar (D_i, V_i) a una potencia, en el que la potencia es la inversa de una clave pública de la entidad firmante (M, I).

11. Método, según cualquiera de las reivindicaciones precedentes, en el que un bono electrónico firmado (V_i) comprende un bono electrónico sin firmar (V_i^*) y la firma del emisor (S_I) en el bono electrónico sin firmar (V_i^*).

12. Método de utilización de un bono electrónico (V_i) generado por el método, según cualquiera de las reivindicaciones precedentes, comprendiendo el método las etapas de:

- el usuario (U) entrega el bono electrónico (V_i) a un comerciante (M),
- el comerciante verifica si el bono electrónico incluye la firma (S_I) del emisor (I), y
- el comerciante (M) únicamente proporciona bienes o servicios si el bono electrónico (V_i) incluye dicha firma (S_I) del emisor (I).

13. Método, según la reivindicación 12, en el que la etapa de entrega del bono electrónico (V_i) comprende, además, la entrega bien de un primer valor intermedio (f(a_i+Q)) y de un número aleatorio (a_i) o de un segundo valor intermedio (f(a_i)) y de un valor de suma (a_i+Q), a efectos de determinar la identificación (Q) del usuario (U) cuando se recibe el mismo bono (V_i) más de una vez.

14. Producto de programa de ordenador para llevar a cabo el método, según cualquiera de las reivindicaciones precedentes.

15. Dispositivo (10) para emitir bonos electrónicos (V_i) que un usuario puede entregar a un comerciante (M) a cambio

de bienes o servicios, comprendiendo el dispositivo:

- una unidad receptora (11) para recibir una declaración electrónica (D_{i-1}) del usuario (U),
- una unidad de verificación (12) para verificar si la declaración electrónica incluye una firma (S_M) del comerciante (M) en un bono electrónico (V_{i-1}^*) anterior, y
- una unidad de emisión (13) para proporcionar una firma (S_I) en un bono electrónico (V_i^*) nuevo únicamente si la declaración electrónica incluye dicha firma (S_M) del comerciante.

16. Dispositivo, según la reivindicación 15, en el que la unidad de emisión (13) proporciona una firma (S_I) en un primer bono electrónico (V_1^*) para el usuario (U) en la ausencia de una declaración (D_{i-1}).

17. Dispositivo, según la reivindicación 15 ó 16, en el que el bono electrónico (V_i^*) contiene la identidad (Q) oculta de el usuario (U).

18. Sistema para proporcionar bienes y/o servicios a cambio de bonos (V_i), comprendiendo el sistema un dispositivo de emisión (10), según cualquiera de las reivindicaciones 15 a 17.

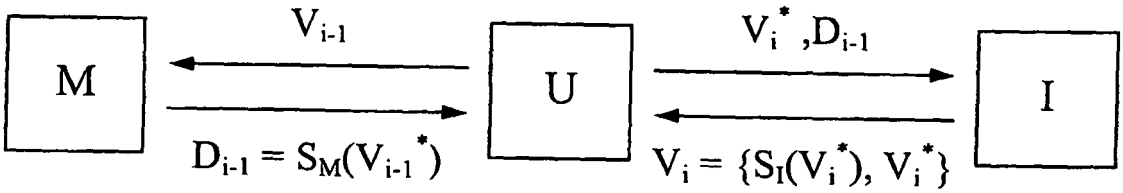
M
U
I
V_{i-1}
$D_{i-1} = S_M(V_{i-1}^*)$
V_i^*, D_{i-1}
$V_i = \{S_I(V_i^*), V_i^*\}$

Fig. 1

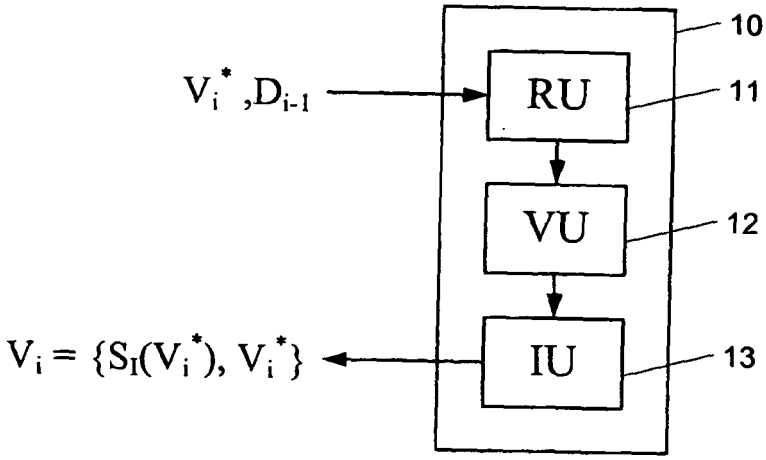
V_i^*, D_{i-1}
RU
VU
IU
$V_i = \{S_I(V_i^*), V_i^*\}$
10
11
12
13

Fig. 2