(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 078**

(21) Número de solicitud: 201431175

(51) Int. CI.:

G06Q 20/32 (2012.01)
H04L 9/00 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

01.08.2014

(43) Fecha de publicación de la solicitud:

01.02.2016

(71) Solicitantes:

UNIVERSITAT POMPEU FABRA (30.0%)
Plaça de la Mercè, 10-12
08002 Barcelona ES;
SIGNORINI, Matteo (30.0%);
DI PIETRO, Roberto (20.0%) y
LOMBARDI, Flavio (20.0%)

(72) Inventor/es:

SIGNORINI, Matteo;
DI PIETRO, Roberto;
LOMBARDI, Flavio y
DAZA, Vanesa

(74) Agente/Representante:

PONTI SALES, Adelaida

(54) Título: **Dispositivo electrónico portátil de moneda**

(57) Resumen:

Dispositivo electrónico portátil de moneda para realizar transacciones monetarias entre un usuario (P) y un vendedor (V), que comprende un elemento de moneda (1) provisto de un selector de moneda (2) para realizar la selección de moneda o monedas a partir de una solicitud del vendedor (V), unos registros de entradas (4) de función (3) destinados a ser seleccionados en función de la selección de moneda o monedas, una función (3) de cálculo de una moneda que a partir de los valores de registros de entrada (4) proporciona una salida de función, unos registros de reconstrucción de salida (5) de función (3), un reconstructor de monedas (6) que a partir de la salida de función y los registros de reconstrucción de salida (5) de función (3) puede reconstruir un valor de moneda original, en el que la función (3) es una función física no clonable borrable de una sola lectura, de modo que no se puede utilizar dos veces la misma moneda. La invención también se refiere a un procedimiento que emplea a este dispositivo.

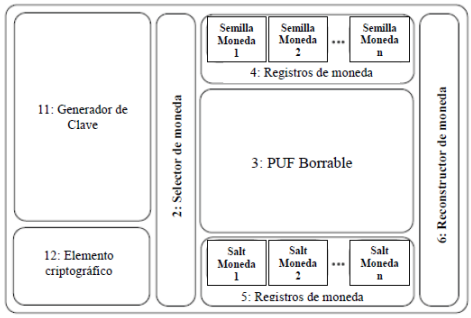


Fig. 3

ES 2 558 078 A1

DESCRIPCIÓN

DISPOSITIVO ELECTRÓNICO PORTÁTIL DE MONEDA

La presente invención se refiere a un dispositivo electrónico portátil de moneda que permite realizar transacciones totalmente fuera de línea (*off-line*) de manera fiable y segura.

Antecedentes de la invención

Actualmente las soluciones de pago digitales se basan en la capacidad de los dispositivos involucrados para operar en línea, es decir, para conectarse a un servicio de pago remoto fiable. Algunos sistemas de pago con tarjeta actuales son fuera de línea (*off-line*), ya que proporcionan una verificación fuera de línea en el punto de venta.

Sin embargo, estos servicios se limitan a la autenticación de usuarios, mientras que se basan a ciegas en la confianza en el banco para las transacciones de los usuarios. Como tales, las transacciones de usuario se pagan / garantizan por parte del banco, incluso en caso de uso indebido.

Sin embargo, para todas aquellas tarjetas que no están ligadas a una cuenta bancaria, como las tarjetas de prepago, el problema principal es que no siempre se dispone de una conexión activa a Internet. Esto puede ser debido a alguna interrupción temporal del servicio de red o a una falta completa de cobertura de la red.

Por último, pero no menos importante, este tipo de soluciones en línea no son muy eficientes debido a los retrasos y problemas de fiabilidad que intervienen en la comunicación remota. Como tal, algunos comerciantes prefieren una solución fuera de línea para aprovechar el aumento de la rapidez y poder beneficiarse de los ahorros en los costes de no utilizar costosos sistemas de transmisión de datos móviles.

Las soluciones propuestas hasta ahora para los pagos móviles se pueden clasificar de acuerdo con las condiciones de conexión de cada dispositivo. Estos se clasifican de acuerdo con todo el enfoque de sistema de pago y no en función de cada dispositivo individual, obteniéndose así la siguiente taxonomía precisa:

Totalmente en línea (*Fully On-Line*): las soluciones como las descritas en [2, 10] hacen que

el dispositivo móvil del usuario se conecte con una red 3G con el fin de comunicarse con el banco u otra puerta de pago;

Semi fuera de línea (*Semi Off-line*): Las soluciones como las descritas en [11,18] requieren una conexión activa procedente sólo del dispositivo de proveedor y no desde el dispositivo del usuario;

Débil fuera de línea (*Weak Off-line*): Las soluciones como las descritas en [4, 14] requieren una conexión ya sea a un conjunto de datos compartido o en una red peer-to-peer. Tal conjunto de datos, que permite el acceso a todas las transacciones anteriores, permite a los proveedores comprobar la validez y los atributos cuenta de usuario, lo cual evita comportamientos maliciosos como los de duplicar el gasto. Otras soluciones pertenecientes a la categoría débil fuera de línea trabajan con dinero en efectivo digital diseñado para ser aceptado, ya sea por un proveedor específico (por ejemplo, cupones) o dentro de una ventana de corta duración específica como en [1, 15]; Otra solución de estas se describe en [5] que describe un uso fuera de línea, pero que aprovecha un componente remoto para almacenar y administrar las claves. La presencia de una tarjeta [7] requiere una conexión a un sistema remoto con el fin de transmitir los registros de compra en un punto posterior en el tiempo. También en [8] Se necesita un servidor remoto para validar las claves. Como tal, esto no puede considerarse una solución completamente desconectado.

Completamente fuera de línea (*Fully Off-Line*): Son soluciones que no requieren ninguna conexión de red externa, pero asumen que tanto el usuario como los dispositivos de vendedores son de confianza [9].

Además, en [6] es un documento de patente que reivindica garantizar la confianza del terminal POS.

Por lo tanto, los inconvenientes limitaciones principales de las soluciones del estado de la técnica son las siguientes:

Partes de confianza (*Trusted-parties*): tanto el usuario como el dispositivo de proveedor se suponen de confianza.

Ventana Temporal (*Time-Window*): un aspecto importante de las soluciones fuera de línea es que el permiso de cuenta de usuario para hacer compras puede ser invalidado sin que el

vendedor lo sepa. Una posible solución es comprobar con frecuencia y validar la renovación del permiso por parte del banco.

Con las soluciones completamente fuera de línea, se plantea la cuestión relativa a la forma de hacer el seguimiento de las transacciones pasadas. De hecho, un vendedor fuera de línea no puede comprobar fácilmente si algunas monedas digitales ya se han gastado o no.

Esta es la principal razón por la que las soluciones propuestas hasta ahora en la literatura requieren algún tipo de tercero de confianza (*Trusted Third Party* - TTP) para almacenar las transacciones pasadas y comprobar dicha lista cuando se recibe una nueva solicitud de pago (verificación en tiempo real) o cuando la solicitud se ha realizado (verificación aplazada). En las soluciones de verificación aplazadas, el vendedor sólo comprueba la identidad del usuario, mientras que el pago se notificará al banco en un momento posterior. A diferencia de las soluciones aplazadas, en los enfoques en tiempo real el dinero se transfiere cuando se realiza la transacción. Sin embargo, en ambos casos se necesita un TTP con el fin de evitar los ataques de doble gasto mediante la comprobación de las transacciones pasadas con otros vendedores.

Finalmente son conocidos los sistemas de pago electrónicos que tienen alojada una moneda en una función. Por ejemplo, en EP2684331 se describe un sistema de pago electrónico que utiliza una moneda electrónica, pero en el cual la condición de borrable depende de la confianza en un software/firmware incrustado. En este caso, la propiedad de evidencia de manipulación se supone para varios de sus componentes. Incluso el puerto de comunicaciones I/O, la interfaz USB y varios otros componentes se suponen de confianza. Incluso la memoria en la que se almacenan las monedas se supone de confianza. Asimismo, el protocolo descrito no es del todo fuera de línea, puesto que en algún momento se deben actualizar listas de CRLs para verificar la validez de nuevas monedas digitales.

Descripción de la invención

Para superar los inconvenientes citados, la presente invención propone un dispositivo electrónico portátil de moneda para realizar transacciones monetarias entre un usuario y un vendedor, que comprende un elemento de identidad y un elemento de moneda, estando provisto el elemento de moneda de:

- Un generador de clave destinado a calcular sobre la marcha una clave privada del

elemento de moneda;

- Un elemento criptográfico destinado a realizar las operaciones de cifrado y descifrado a partir de la clave privada del elemento de moneda, en particular destinada a descifrar la solicitud del elemento de identidad y a cifrar la respuesta del elemento de moneda antes de enviarla al elemento de identidad;
- Un selector de moneda para realizar la selección de moneda o monedas a partir de una solicitud del elemento de identidad;
- Unos registros de entradas de función destinados a ser seleccionados en función de la selección de moneda o monedas;
- Una función de cálculo de una moneda que a partir de los valores de registros de entrada proporciona una salida de función;
- Unos registros de reconstrucción de salida de función;
- Un reconstructor de monedas que a partir de la salida de función y los registros de reconstrucción de salida de función puede reconstruir un valor de moneda original;

que se caracteriza por el hecho de que la función es una función física no clonable borrable de una sola lectura para cada registro de entrada, de modo que no se puede utilizar dos veces la misma moneda.

Preferentemente, el elemento de identidad del usuario está provisto de:

- Un generador de clave destinado a calcular sobre la marcha una clave privada del elemento de identidad;
- Un elemento criptográfico destinado a realizar las operaciones de cifrado y descifrado a partir de la clave privada del elemento de identidad, en particular destinada a descifrar la solicitud del vendedor, a cifrar la respuesta del usuario antes de enviarla al vendedor, a cifrar la solicitud de ser enviado al elemento de moneda y a descifrar la respuesta obtenida a partir del elemento de moneda.

Ventajosamente, ambos generadores de claves que se encuentran en el elemento de moneda y de identidad contienen una función física no clonable no borrable. En este caso, sí que la función puede ser utilizada varias veces con el mismo valor de entrada.

La invención también se refiere a un procedimiento para realizar transacciones monetarias entre un usuario y un vendedor utilizando un dispositivo electrónico provisto de un elemento de moneda y de un elemento de identidad, donde el elemento de moneda está provisto de:

- Un selector de moneda;
- Unos registros de entradas de función;
- Una función de cálculo de una moneda que es una función física no clonable borrable de una sola lectura;
- Unos registros de reconstrucción de salida de función;
- Un reconstructor de monedas;
- Un generador de clave;
- Un elemento criptográfico;

Mientras, el elemento de identidad está provisto de:
- Un generador de clave;
- Un elemento criptográfico;

Comprendiendo el procedimiento las etapas de:

a) Realizar una solicitud de transacción al vendedor por parte del usuario;
b) Generar una solicitud de moneda por parte del vendedor;
c) Cifrar con la clave pública del elemento de identidad del usuario la solicitud de moneda por parte del vendedor;
d) Enviar al elemento de identidad del usuario por parte del vendedor la solicitud de moneda;
e) Por parte del elemento de identidad, calcular sobre la marcha la clave privada del elemento de identidad mediante el generador de clave;
f) Descifrar la solicitud del vendedor con la clave privada del elemento de identidad;
g) Cifrar con la clave pública del elemento de moneda la solicitud de moneda por parte del elemento de identidad;
h) Por parte del elemento de moneda, calcular sobra la marcha la clave privada del elemento de moneda mediante el generador de clave;
i) Enviar la solicitud del elemento de identidad al elemento de moneda;
l) Descifrar la solicitud del elemento de identidad por parte del elemento de moneda;
m) Realizar la selección registros de entradas de función mediante el selector de moneda;
n) Aplicar a la función estos registros, para obtener una salida de función;
o) Reconstruir las monedas mediante el reconstructor de monedas a partir de la salida de la función y los registros de reconstrucción de salida de función;
p) Por parte del elemento de moneda, cifrar la moneda reconstruida con la clave publica del elemento de identidad mediante el elemento criptográfico;

q) Enviar la moneda reconstruida al elemento de identidad;

r) Descifrar la moneda reconstruida del elemento de moneda por parte del elemento de identidad;

s) Cifrar la moneda reconstruida con el valor aleatorio SALT y la clave privada del elemento de identidad;

t) Enviar al vendedor la moneda reconstruida por parte del usuario;

u) Descifrar por parte del vendedor la moneda recibida del usuario;

Las etapas e) h) n) se realiza con una función física no clonable no borrable.

Breve descripción de las figuras

Para mejor comprensión de cuanto se ha expuesto se acompañan unos dibujos en los que, esquemáticamente y tan sólo a título de ejemplo no limitativo, se representa un caso práctico de realización de la invención.

La figura 1 es un esquema general de arquitectura de dispositivo de usuario que muestra todos los tipos posibles que se pueden conseguir con el elemento de moneda;

La figura 2 es un esquema general de arquitectura de las dos partes según la invención;

La figura 3 es una arquitectura de elemento de moneda según la invención;

La figura 4 es una arquitectura de elemento de identidad;

La figura 5 es una arquitectura de elemento de generador de clave;

La figura 6 muestra la reconstrucción de moneda en el elemento de moneda del pagador;

La figura 7 es la arquitectura de bloque de Función Física No clonable;

La figura 8 muestra el protocolo de pago según la invención.

La figura 9 muestra el detalle de la etapa 6 de la figura 8.

Descripción de una realización preferida

Tal como puede apreciarse en las figuras 3 y 4, la presente invención propone un dispositivo electrónico portátil para realizar transacciones monetarias entre un usuario P y un vendedor V, que comprende un elemento de moneda 1 y un elemento de identidad 7. El elemento de moneda 1 está provisto de

- Un generador de clave 11 destinado a calcular sobre la marcha una clave privada CESK del elemento de moneda 1, comprendiendo este generador una función física no clonable no borrable;
- Un elemento criptográfico 12 destinado a realizar las operaciones de cifrado y descifrado, en particular destinado a descifrar la solicitud del elemento de identidad 7 con la clave CESK y a cifrar con la clave IEPK la respuesta del elemento de moneda 1 antes de enviarla al elemento de identidad 7;
- Un selector de moneda 2 para realizar la selección de moneda o monedas a partir de una solicitud del elemento de identidad 7;
- Unos registros de entradas 4 de función 3 destinados a ser seleccionados en función de la selección de moneda o monedas;
- Una función 3 de cálculo de una moneda que a partir de los valores de registros de entrada 4 proporciona una salida de función;
- Unos registros de reconstrucción de salida 5 de función 3;
- Un reconstructor de monedas 6 que a partir de la salida de función y los registros de reconstrucción de salida 5 de función 3 puede reconstruir un valor de moneda original;

caracterizado por el hecho de que la función 3 es una función física no clonable borrable de una sola lectura para cada registro de entrada, de modo que no se puede utilizar dos veces la misma moneda.

Tal como puede apreciarse en la figura 4, el dispositivo comprende un elemento de identidad 7 del usuario que comprende:

- Un generador de clave 71 destinado a calcular sobre la marcha una clave privada IESK del elemento de identidad 7, comprendiendo este generador una función física no clonable no borrable;
- Un elemento criptográfico 72 destinado a realizar las operaciones de cifrado y descifrado,

en particular destinado a descifrar la solicitud del vendedor V con la clave privata IESK, a cifrar la solicitud del elemento de moneda con la clave CEPK, a descifrar la respuesta del elemento de moneda con la clave IESK y a cifrar con el valor aleatorio SALT y la clave IESK la respuesta del usuario P antes de enviarla al vendedor V.

Tal como puede apreciarse en la figura 8, la invención también se refiere a un procedimiento para realizar transacciones monetarias entre un usuario P y un vendedor V utilizando un dispositivo electrónico provisto de un elemento de identidad 7 y un elemento de moneda 1, estando el elemento de moneda 1 provisto de:

- Un generador de clave 11;
- Un elemento criptografico 12;
- Un selector de moneda 2;
- Unos registros de entradas 4 de función 3;
- Una función 3 de cálculo de una moneda que es una función física no clonable borrable de una sola lectura;
- Unos registros de reconstrucción de salida 5 de función 3;
- Un reconstructor de monedas 6;

Estando el elemento de identidad 7 provisto de:

- Un generador de clave 71;
- Un elemento criptográfico 72;

Comprendiendo el procedimiento las etapas de:

a) Realizar una solicitud de transacción al vendedor V por parte del usuario P;

b) Generar una solicitud de moneda por parte del vendedor V;

c) Cifrar con la clave pública IEPK del elemento de identidad del usuario P la solicitud de moneda por parte del vendedor V;

d) Enviar al elemento de identidad del usuario P por parte del vendedor V la solicitud de moneda;

e) Por parte del elemento de identidad, calcular sobre la marcha la clave privada IESK del elemento de identidad mediante el generador de clave 71;

f) Descifrar la solicitud del vendedor con la clave IESK;

g) Cifrar con la clave publica del elemento de moneda CEPK la solicitud de moneda por parte del elemento de identidad;

h) Enviar la solicitud del elemento de identidad al elemento de moneda 1;

i) Por parte del elemento de moneda, calcular sobra la marcha la clave privada del elemento de moneda CESK mediante el generador de clave;

l) Descifrar la solicitud del elemento de identidad por parte del elemento de moneda;

m) Realizar la selección registros de entradas 4 de función 3 mediante el selector de moneda 2;

n) Aplicar a la función 3 estos registros 4, para obtener una salida de función;

o) Reconstruir las monedas mediante el reconstructor de monedas 6 a partir de la salida 7 de la función 3 y los registros de reconstrucción de salida 5 de función 3;

p) Cifrar la moneda reconstruida con la clave publica del elemento de identidad IEPK por parte del elemento de moneda mediante el elemento criptográfico 12;

q) Enviar la moneda reconstruida al elemento de identidad 7;

r) Descifrar con la clave IESK la moneda reconstruida del elemento de moneda por parte del elemento de identidad;

s) Cifrar con el valor aleatorio SALT y la clave IESK la moneda reconstruida por parte del elemento de identidad;

t) Enviar al vendedor V la moneda reconstruida por parte del usuario P;

u) Descifrar por parte del vendedor V y con la clave IEPK la moneda recibida del usuario P

La etapa e) i) n) se realiza con una función física no clonable no borrable.

La figura 1 muestra las diferentes maneras en las se puede implementar un elemento de moneda (también conocido como tarjeta de pago).

Como dispositivo externo, el elemento de moneda (o dispositivo electrónico portátil de moneda) puede ser implementado como un dispositivo USB dedicado o una tarjeta SD o incluso como un dispositivo remoto situado en la nube.

Como dispositivo interno, el elemento de moneda puede ser implementado como un elemento seguro. El elemento de moneda ha sido diseñado como un componente separado para bloquear las actividades maliciosas de usuarios mientras proporciona la privacidad del usuario P. Mediante el uso de un elemento de identidad 7 para identificar el dispositivo pagador P implicado en el pago, un dispositivo de usuario malicioso puede ser añadido, por parte del emisor del elemento de moneda, a una lista negra de usuarios. Como tal, independientemente de qué elemento de moneda se utilice en una transacción, no se permitirá completar la transacción a un dispositivo de usuario que esté en la lista negra.

La figura 2 muestra todos los elementos que intervienen en un caso de aplicación de la invención. Suele haber dos involucrados en un protocolo de pago. El dispositivo pagador P que se compone de un elemento de identidad y de un elemento de moneda y tambien un dispositivo de beneficiario V, que será el vendedor.

A partir de ahora se denominará PUF (por sus siglas en inglés *Physical Unclonable Function*) a la Función Física No clonable. Esta puede seleccionarse como borrable o no borrable tal como se verá en lo sucesivo.

La Figura 3 muestra en detalle la arquitectura interna de un dispositivo de elemento de moneda. Dicho dispositivo está compuesto por:

Un generador de clave 11: este se encarga de calcular la clave secreta del elemento de moneda en tiempo de ejecución;

Un elemento criptografico 12: este se encarga de de todas las operaciones de cifrado y descifrado;

Un selector de monedas 2: es responsable de la selección de los registros 4, 5 adecuados utilizados para calcular el valor de salida calculado por la PUF borrable con el fin de obtener el valor final de la moneda;

PUF Borrable 3: es una PUF con una característica de una sola lectura para cada moneda. Después de la primera interrogación, si se utiliza la misma entrada, la salida será aleatoria;

Registros de moneda de entrada 4 y de salida 5: se utilizan para almacenar tanto las entradas 4 a la PUF 3 y los valores re reconstrucción de salida 5 necesarios para reconstruir el valor de la moneda original;

Reconstructor de Moneda 6: es responsable de utilizar tanto la salida procedente de la PUF y registros de monedas 5 con el fin de reconstruir el valor original de la moneda.

La figura 4 muestra los dos componentes del elemento de identidad 7. Dicho dispositivo está compuesto por:

Generador de clave 71: se utiliza para calcular la clave secreta del elemento de identidad en

tiempo de ejecución;

Elemento criptografico 72: se utiliza para operaciones de cifrado / descifrado.

La Figura 5 muestra el algoritmo de corrección de errores propuesto en [21] y utilizado preferentemente por el dispositivo y el procedimiento de la presente invención para calcular la clave secreta (privada). Este algoritmo se ha usado tanto en el elemento de identidad en la de moneda. La PUF de suma 64 básica consulta la diferencia entre dos términos de retardo, cada uno producido por la suma de 64 valores de PUF. El bit de interrogación C_i de desafío para cada una de las 64 etapas determina qué parte de PUF se utiliza para calcular el término de retardo superior, y cual se utiliza para calcular el término de retardo inferior. El bit de signo de la diferencia entre los dos términos de retardo determina si la PUF da salida a un bit '1 'o '0' para la interrogación de 64 bits $C_0...C_n$. Los bits restantes de la diferencia determinan el nivel de confianza del bit de salida '1 'o '0'. La PUF de suma k puede considerarse como un árbitro PUF (ver [13]) de K etapas con una salida de valor real que contiene tanto el bit de salida, así como su nivel de confianza.

Esta información es utilizada por el bloque de corrección de error de peso ligero dispuesto aguas abajo que es capaz de proporcionar una clave criptográfica tanto al elemento de identidad 7 como al elemento de moneda 1. Mediante el uso de tal proceso de generación de claves criptográficas sobre la marcha ("*on-the-fly*"), ventajosamente según la presente invención no se almacenan claves privadas en el propio elemento evitando y así el espionaje / lectura pro parte de usuarios malintencionados y garantizándose que sólo el elemento de identidad / moneda correcto puede calcular su propia clave privada.

La figura 6 muestra cómo se reconstruye la moneda en el elemento de moneda. En primer lugar se calcula la clave secreta con el fin de entender la solicitud recibida por el elemento de identidad del pagador P. La solicitud deberá contener el número de monedas a leer junto con otros valores efímeros. Cada número de moneda que se encuentra en la solicitud se utilizará como entrada a un selector de monedas 2 que va a leer un registro de moneda 4 especial que contiene la entrada a la PUF 3 que se utilizará para esa moneda específica. Este número de moneda también se utilizará como entrada a un segundo registro 5 de la moneda que contiene un valor de moneda (registros de reconstrucción de moneda) que se combinará con la salida de la PUF 3 con el fin de reconstruir el valor de la moneda original diseñada por el emisor del elemento de moneda.

La figura 7 muestra el algoritmo y arquitectura que se utilizan para la generación de la clave privada. Este elemento se utiliza tanto en el elemento de moneda como en el elemento de identidad

La figura 8 muestra el protocolo de transacción según la presente invención. En este diagrama de flujo las referencias tienen los siguientes significados:

Salt	Valor Salt
CEPK	Clave pública del elemento de moneda
CESK	Clave secreta (privada) del elemento de moneda
IEPK	Clave pública del elemento de identidad
IESK	Clave secreta (privada) del elemento de identidad
EReq	Solicitud de beneficiario cifrada
Req	Solicitud de beneficiario
DEC	Descifrar
ENC	Cifrar
CoinVal	Valor de moneda
CreditVal	Valor del crédito
CreditIdx	Créditos disponibles
SCID	Scratch Card ID
ERes	Respuesta de pago cifrada
Res	Respuesta de pago
BPK	Clave pública del Banco (Bank Public Key)

La figura 9 describe con detalle todas etapas de la fase 6 de la figura 8. En estas etapas los elementos de identidad y de moneda utilizan sus propias claves privada/ pública para comunicar de forma segura el valor de moneda a y desde el elemento de moneda.

Por lo tanto, se ha descrito un nuevo enfoque de pago electrónico que supera las soluciones anteriores con respecto a la flexibilidad y la seguridad. De hecho, el dispositivo y el procedimiento de la presente invención no exigen ningún tipo de conectividad de red o de un tercero de confianza.

Según la presente invención, tanto el dispositivo de beneficiario como de pagador se pueden desconectar de Internet o de cualquier otro tercero de confianza, al poderse confiar únicamente en los datos locales integrados. Este es el primer enfoque que proporciona

pagos totalmente fuera de línea seguros resistentes contra un adversario omnipresente que es incluso capaz de ajustar todos los dispositivos que intervienen en el proceso de pago.

Para lograr este objetivo, la presente invención saca partido de las nuevas funciones físicas no clonables (PUF). La mayoría de las PUF se había utilizado en el pasado para proporcionar una autenticación de usuario más fuerte. Sin embargo, una de las características más importantes de las PUF es su capacidad a prueba de intrusión.

En los últimos años, se han introducido otras soluciones de pago de tarjetas inteligentes basadas en hardware a prueba de manipulaciones. Sin embargo, el enfoque propuesto sólo supone que un pequeño componente del dispositivo al que pertenece la PUF es a prueba de intrusión (proporcionada por el PUF).

Como consecuencia, los supuestos de la presente invención son mucho menos restrictivos y más realistas que con otros enfoques. Además, la presente invención es la primera solución que no se basa en transacciones aplazadas. Un enfoque pospuesto, adoptado por la mayoría de las soluciones de pago de tarjetas de crédito actuales, es capaz de verificar la identidad del usuario en tiempo de ejecución, pero requiere que la tarjeta de crédito se conecte a una cuenta bancaria desde donde se cogerá el dinero.

Según la presente invención, el pago se realiza en tiempo de ejecución y no se requieren acciones postergadas. La falta de conectividad a cualquier cuenta bancaria también hace que la presente invención sea interesante desde el punto de vista de la privacidad de las transacciones del usuario. De hecho, a diferencia de otras soluciones, según la presente invención el elemento de la moneda se puede comprar sin aportar ningún documento de identificación.

A pesar de que se ha hecho referencia a una realización concreta de la invención, es evidente para un experto en la materia que el dispositivo y el procedimiento descritos son susceptibles de numerosas variaciones y modificaciones, y que todos los detalles mencionados pueden ser sustituidos por otros técnicamente equivalentes, sin apartarse del ámbito de protección definido por las reivindicaciones adjuntas.

Referencias

[1] M. Aigner, S. Dominikus, and M. Feldhofer. A System of Secure Virtual Coupons Using NFC Technology. In Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07), pages 362– 366. IEEE, 2007.

[2] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H. Chiu. Using 3G network components to enable NFC mobile transactions and authentication. In Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on, volume 1, pages 441 –448, Dec 2010.

[3] X. Dai, O. Ayoade, and J. Grundy. Off-line micro-payment protocol for multiple vendors in mobile commerce. In Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on, pages 197–202, 2006.

[4] S. Dominikus and M. Aigner. mCoupons: An Application for Near Field Communication (NFC). In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, pages 421–428, 2007.

[5] P. C. EHLINGER, JR. In-card access control and monotonic counters for offline payment processing ssytem, 06 2006.

[6] P. C. EHLINGER, JR. Point of sale terminal having enhanced security, 06 2006.

[7] P. C. EHLINGER, JR. Presence-of-card code for offline payment processing system, 06 2006.

[8] P. C. EHLINGER, JR. Transaction signature for offline payment processing system, 06 2006.

[9] C.-I. Fan, Y.-K. Liang, and C.-N. Wu. An anonymous fair offline micropayment scheme. In Information Society (i-Society), 2011 International Conference on, pages 377 –381, 2011.

[10] S. Golovashych. The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals. In Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2005. IDAACS 2005. IEEE,

pages 407–412, Sep 2005.

[11] K. S. Kadambi, J. Li, and A. H. Karp. Near-field communication-based secure mobile payment service. In ICEC ’09: Proceedings of the 11th International Conference on Electronic Commerce. ACM Request Permissions, Aug 2009.

[12] S. Kim and W. Lee. A pay word-based micropayment protocol supporting multiple payments. In Computer Communications and Networks, 2003. ICCCN 2003. Proceedings. The 12th International Conference on, pages 609–612, 2003.

[13] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk, and S. Devadas. Extracting secret keys from integrated circuits. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, 13(10):1200–1205, 2005. 11

[14] T. Nishide and K. Sakurai. Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited. In Proceedings of the 2011 Third International Conference on Intelligent Networking and Collaborative Systems, INCOS ’11, pages 656–661, Washington, DC, USA, 2011. IEEE Computer Society.

[15] V. Patil and R. K. Shyamasundar. An efficient, secure and delegable micropayment system. In e-Technology, e-Commerce and e-Service, 2004. EEE ’04. 2004 IEEE International Conference on, pages 394–404, 2004.

[16] C. Popescu and H. Oros. An off-line electronic cash system based on bilinear pairings. In Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services. 14th International Workshop on, pages 438–440, 2007.

[17] R. L. Rivest. Payword and micromint: two simple micropayment schemes. In CryptoBytes, pages 69–87, 1996.

[18] V. C. Sekhar and S. C. Mrudula. A complete secure customer centric anonymous payment in a digital ecosystem. Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on.

[19] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar. Credit card fraud detection using

hidden markov model. IEEE Transactions on Dependable and Secure Computing, 5(1):37–48, 2008.

[20] C. Wang and R. Lu. An ID-based transferable off-line e-cash system with revokable anonymity. In Electronic Commerce and Security, 2008 International Symposium on, pages 758–762, 2008.

[21] M.-D. M. Yu, D. M'Raihi, R. Sowell, and S. Devadas. Lightweight and secure PUF key storage using limits of machine learning. In Proceedings of the 13th International Conference on Cryptographic Hardware and Embedded Systems, CHES'11, pages 358–373, Berlin, Heidelberg, 2011. Springer-Verlag.

[22] W. Zhan-gang and W. Zhen-kai. A secure off-line electronic cash scheme based on ECDLP. In Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on, volume 2, pages 30–33, 2009.

[23] L. Zhang, J. Yin, and M. Li. A novel off-line anonymous and divisible digital cash protocol utilizing smart card for mobile payment. In Communications and Networking in China, 2006. ChinaCom '06. First International Conference on, pages 1 –6, oct. 2006.

[24] X. Zhou. Threshold cryptosystem based fair off-line e-cash. In Intelligent Information Technology Application, 2008. IITA '08. Second International Symposium on, volume 3, pages 692–696, 2008.

[25] Y. Zongkai, L.Weimin, and T. Yunmeng. A new fair micropayment system based on hash chain. In e-Technology, e-Commerce and e-Service, 2004. EEE '04. 2004 IEEE International Conference on, pages 139–145, 2004.

REIVINDICACIONES

1. Dispositivo electrónico portátil de moneda para realizar transacciones monetarias entre un usuario (P) y un vendedor (V), que comprende un elemento de moneda (1) provisto de

- Un generador de clave (11) destinado a calcular sobre la marcha una clave privada (CESK) del elemento de moneda (1);
- Un elemento criptográfico (12) destinado a realizar las operaciones de cifrado y descifrado, en particular destinado a descifrar con la clave CESK la solicitud del elemento de indentidad y a cifrar con la clave IEPK la respuesta del elemento de moneda antes de enviarla al elemento de identidad;
- Un selector de moneda para realizar la selección de moneda o monedas a partir de una solicitud del elemento de identidad;
- Un selector de moneda (2) para realizar la selección de moneda o monedas a partir de una solicitud del elemento de identidad;
- Unos registros de entradas (4) de función (3) destinados a ser seleccionados en función de la selección de moneda o monedas;
- Una función (3) de cálculo de una moneda que a partir de los valores de registros de entrada (4) proporciona una salida de función;
- Unos registros de reconstrucción de salida (5) de función (3);
- Un reconstructor de monedas (6) que a partir de la salida de función y los registros de reconstrucción de salida (5) de función (3) puede reconstruir un valor de moneda original;

caracterizado por el hecho de que la función (3) es una función física no clonable borrable de una sola lectura para cada registro de entrada, de modo que no se puede utilizar dos veces la misma moneda.

2. Dispositivo según la reivindicación 1, que comprende un elemento de identidad (7) del usuario (P) que comprende:

- Un generador de clave (71) destinado a calcular sobre la marcha una clave privada (IESK) del elemento de identidad (7);
- Un elemento criptográfico (72) destinado a realizar las operaciones de cifrado y descifrado, en particular destinado a descifrar la solicitud del vendedor (V) con la clave privata (IESK), a cifrar la solicitud del elemento de moneda con la clave publica (CEPK), a descifrar la

respuesta del elemento de moneda con la clave privada (IESK) y a cifrar con el valor aleatorio SALT y la clave privada (IESK) la respuesta del usuario P antes de enviarla al vendedor V.

3. Dispositivo según la reivindicación 2, en el que ambos generadores de claves que se encuentran en el elemento de moneda y de identidad contienen una función física no clonable no borrable.

4. Procedimiento para realizar transacciones monetarias entre un usuario (P) y un vendedor (V) utilizando un dispositivo electrónico provisto de un elemento de moneda y de un elemento de identidad (1), estando el elemento de moneda (1) provisto de:

- Un generador de clave (11);
- Un elemento criptográfico (12);
- Un selector de moneda (2);
- Unos registros de entradas (4) de función (3);
- Una función (3) de cálculo de una moneda que es una función física no clonable borrable de una sola lectura;
- Unos registros de reconstrucción de salida (5) de función (3);
- Un reconstructor de monedas (6);
- Un generador de clave (11);
- Un elemento criptográfico (12);

Mientras, el elemento de identidad (7) esta provisto de:
- Un generador de clave (71);
- Un elemento criptográfico (72);

Comprendiendo el procedimiento las etapas de:

a) Realizar una solicitud de transacción al vendedor (V) por parte del usuario (P);
b) Generar una solicitud de moneda por parte del vendedor (V);
c) Cifrar con la clave pública (IEPK) del elemento de identidad (7) del usuario (P) la solicitud de moneda por parte del vendedor (V);
d) Enviar al elemento de identidad (7) del usuario (P) por parte del vendedor (V) la solicitud de moneda;
e) Calcular sobre la marcha la clave privada (IESK) del elemento de identidad (7) mediante

el generador de clave (71);

f) Descifrar la solicitud del vendedor con la clave privada (IESK) del elemento de identidad (7);

g) Cifrar con la clave publica (CEPK) del elemento de moneda (1) la solicitud de moneda por parte del elemento de identidad (7);

h) Enviar la solicitud del elemento de identidad (7) al elemento de moneda (1);

i) Calcular sobra la marcha la clave privada (CESK) del elemento de moneda (1) mediante el generador de clave (11);

l) Descifrar la solicitud del elemento de identidad (7) por parte del elemento de moneda (1);

m) Realizar la selección registros de entradas (4) de función (3) mediante el selector de moneda (2);

n) Aplicar a la función (3) estos registros (4), para obtener una salida de función;

o) Reconstruir las monedas mediante el reconstructor de monedas (6) a partir de la salida (7) de la función (3) y los registros de reconstrucción de salida (5) de función (3);

p) Cifrar la moneda reconstruida con la clave publica (IEPK) del elemento de identidad (7) mediante el elemento criptográfico (12) del elemento de moneda (1);

q) Enviar la moneda reconstruida al elemento de identidad (7);

r) Descifrar con la clave privada (IESK) en el elemento criptografico (72) la moneda reconstruida del elemento de moneda (1) por parte del elemento de identidad (7);

s) Cifrar con el valor aleatorio SALT y la clave privada (IESK) en el elemento criptografico (72) la moneda reconstruida por parte del elemento de identidad (7);

t) Enviar al vendedor (V) la moneda reconstruida por parte del usuario (P);

u) Descifrar por parte del vendedor (V) la moneda recibida del usuario (P);

5. Procedimiento según la reivindicación 4, en el que las etapas e) i) n) se realiza con una función física no clonable no borrable.

Fig. 1

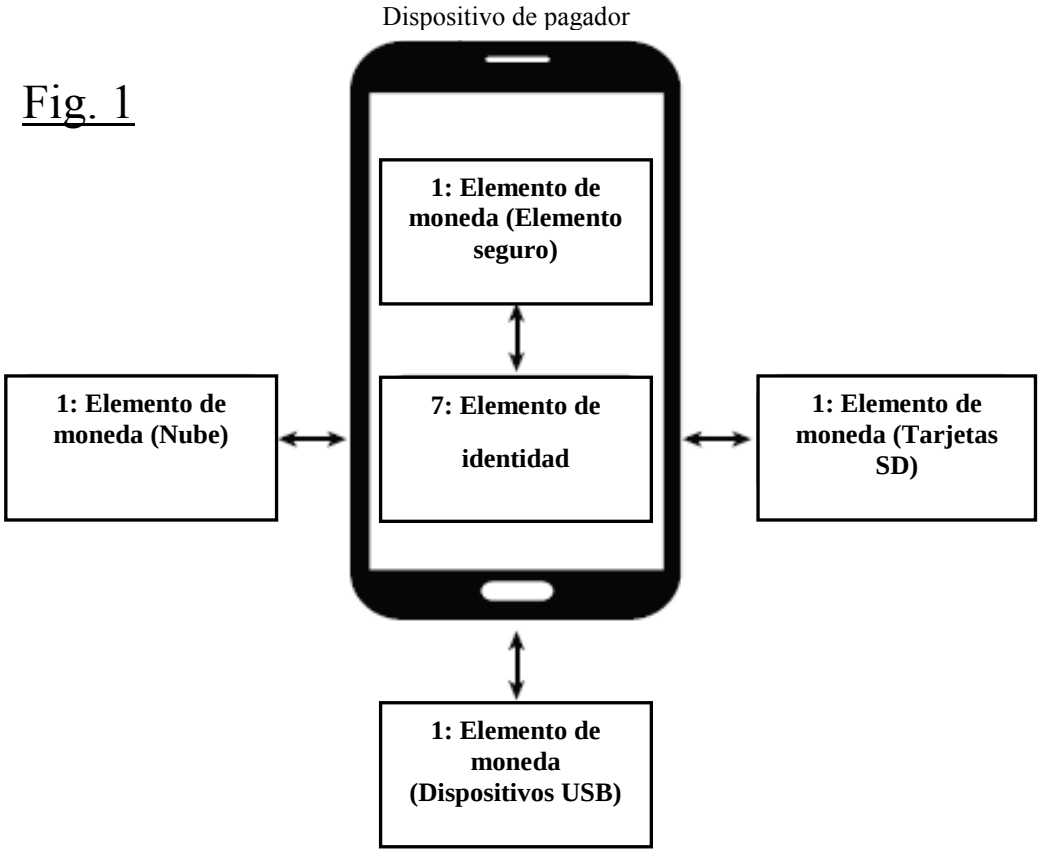
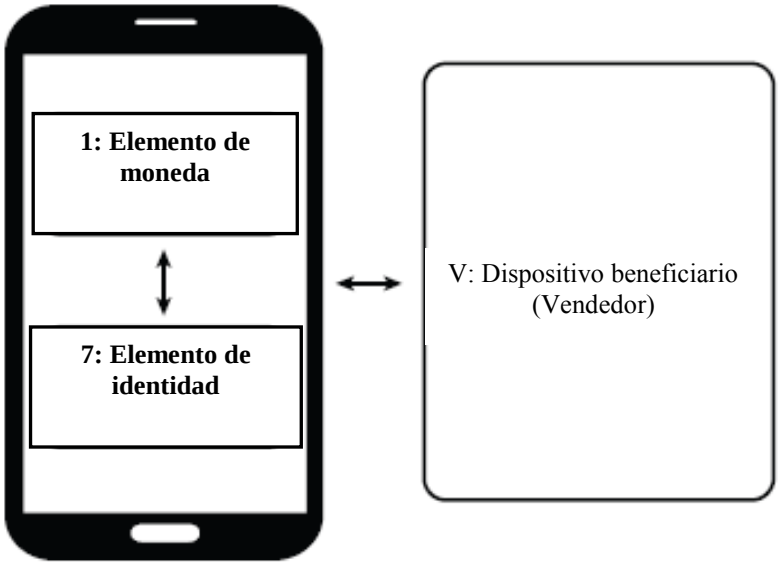

Dispositivo de pagador
1: Elemento de moneda (Elemento seguro)
7: Elemento de identidad
1: Elemento de moneda (Nube)
1: Elemento de moneda (Tarjetas SD)
1: Elemento de moneda (Dispositivos USB)

Fig. 2


1: Elemento de moneda
7: Elemento de identidad
V: Dispositivo beneficiario (Vendedor)
P: Dispositivo de pagador (P)

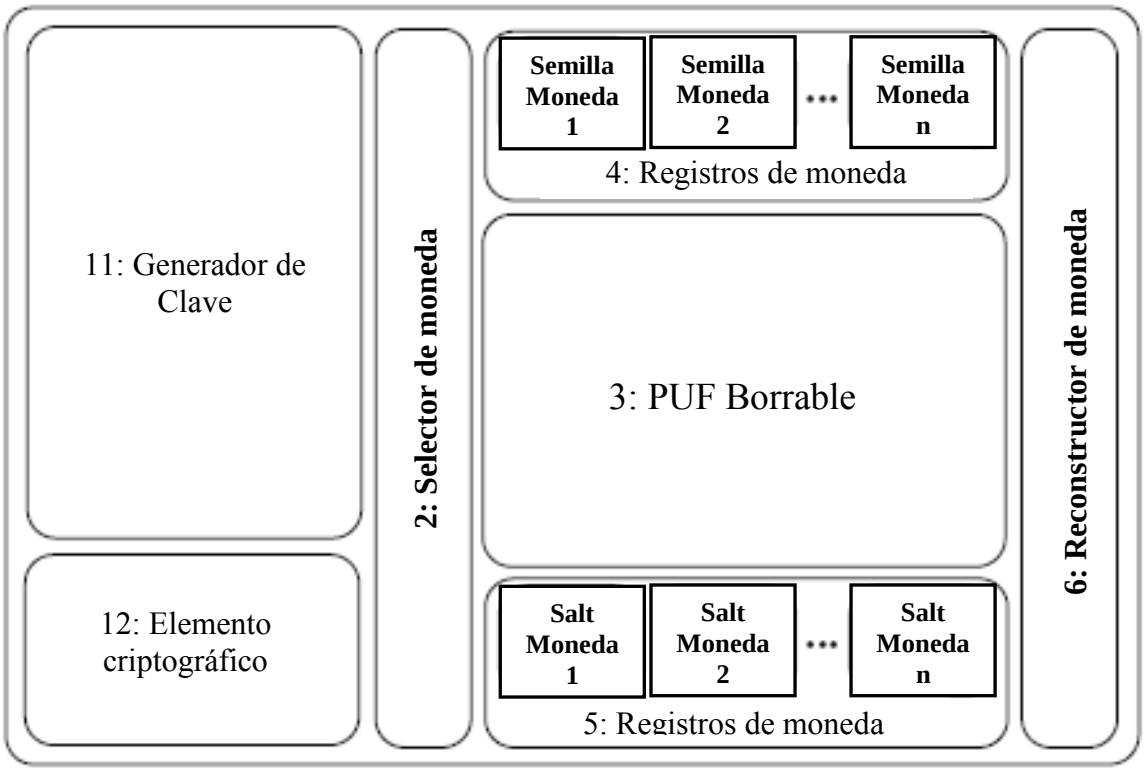

11: Generador de Clave
12: Elemento criptográfico
2: Selector de moneda
Semilla Moneda 1
Semilla Moneda 2
Semilla Moneda n
4: Registros de moneda
3: PUF Borrable
Salt Moneda 1
Salt Moneda 2
Salt Moneda n
5: Registros de moneda
6: Reconstructor de moneda
Elemento de moneda

Fig. 3

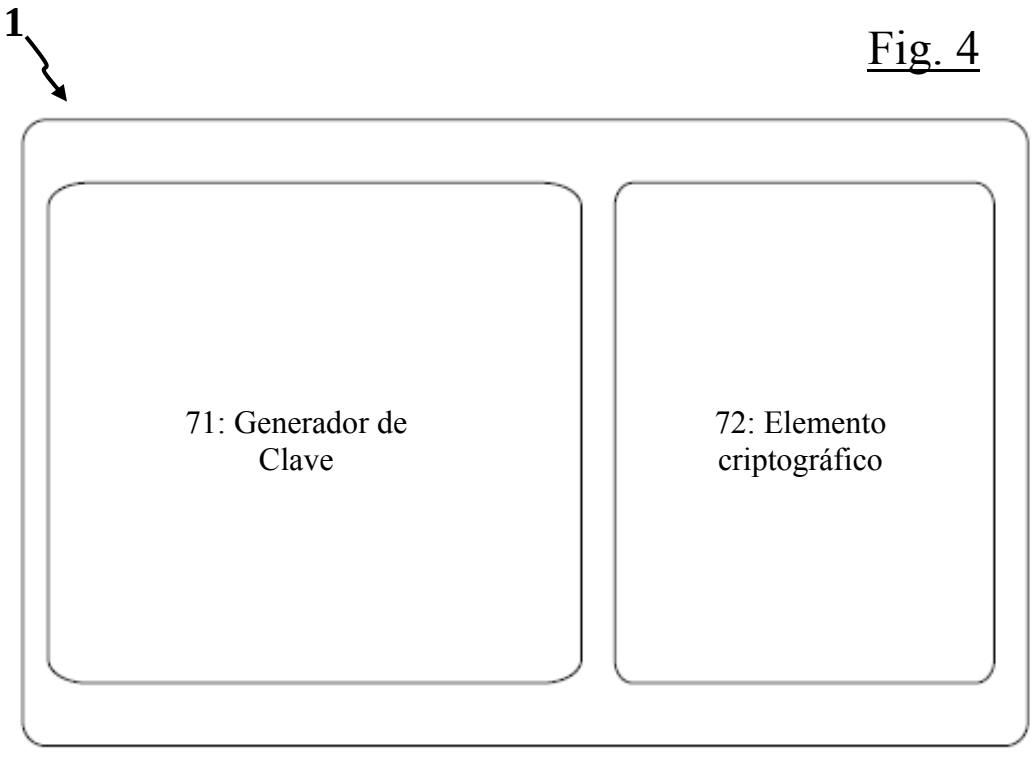

1
71: Generador de Clave
72: Elemento criptográfico
7: Elemento de identidad

Fig. 4

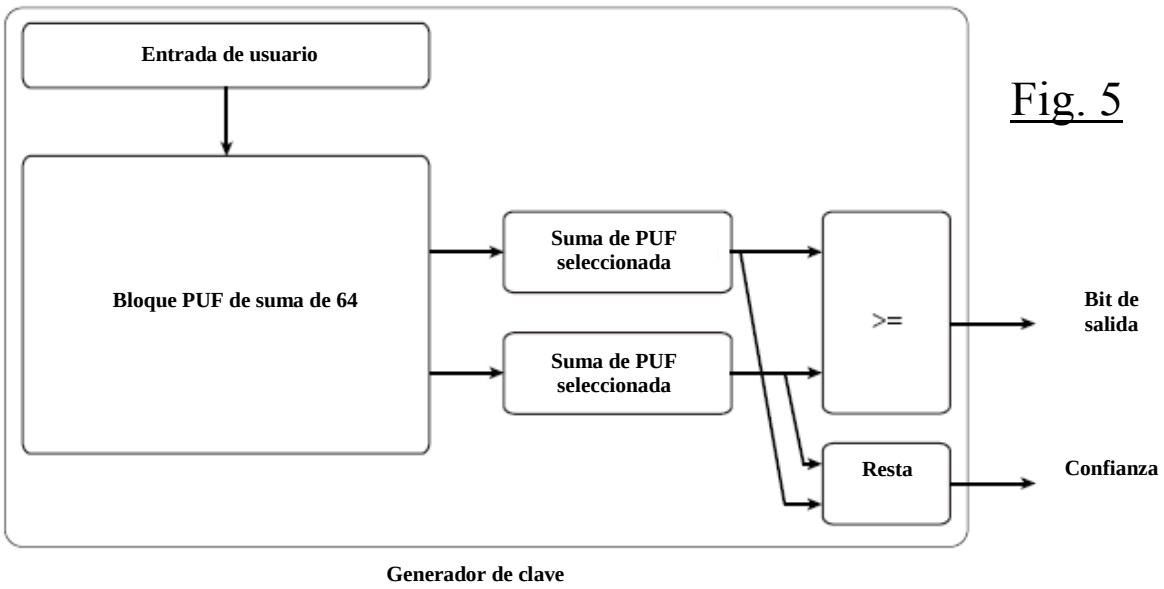

Entrada de usuario
Bloque PUF de suma de 64
Suma de PUF seleccionada
Suma de PUF seleccionada
>=
Resta
Bit de salida
Confianza
Generador de clave

Fig. 5

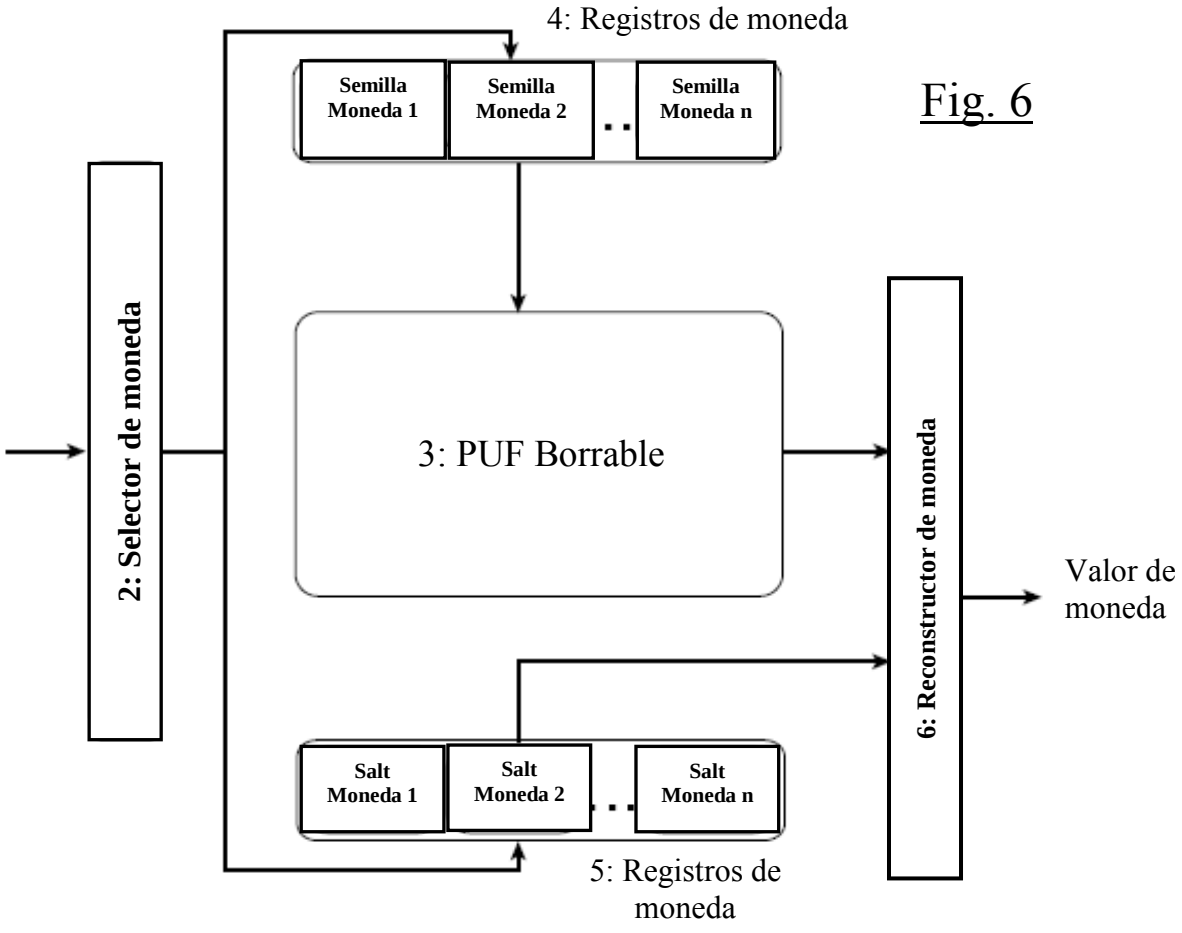
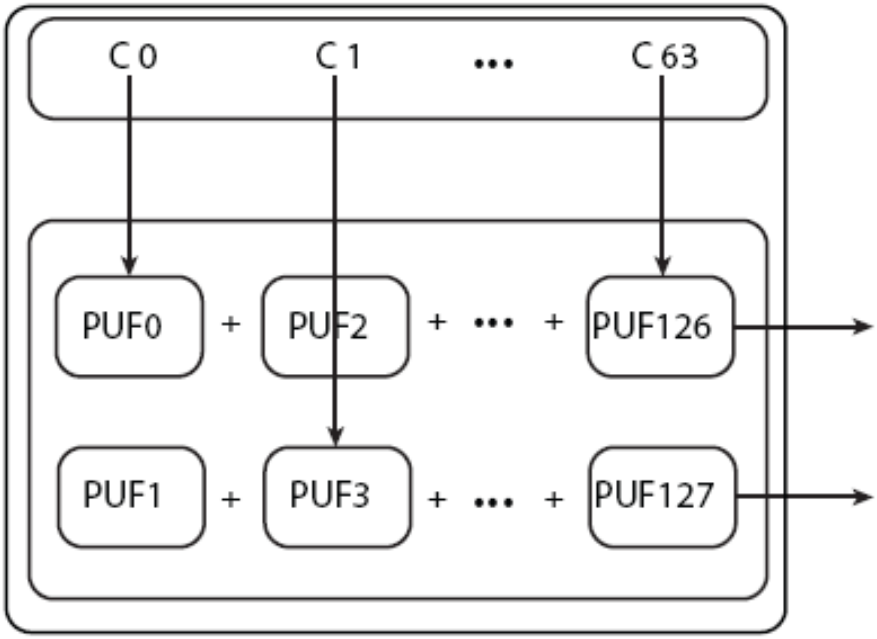

4: Registros de moneda
Semilla Moneda 1
Semilla Moneda 2
Semilla Moneda n
2: Selector de moneda
3: PUF Borrable
6: Reconstructor de moneda
Valor de moneda
Salt Moneda 1
Salt Moneda 2
Salt Moneda n
5: Registros de moneda

Fig. 6



Bloque PUF de Suma
64

Fig. 7

Fig. 8

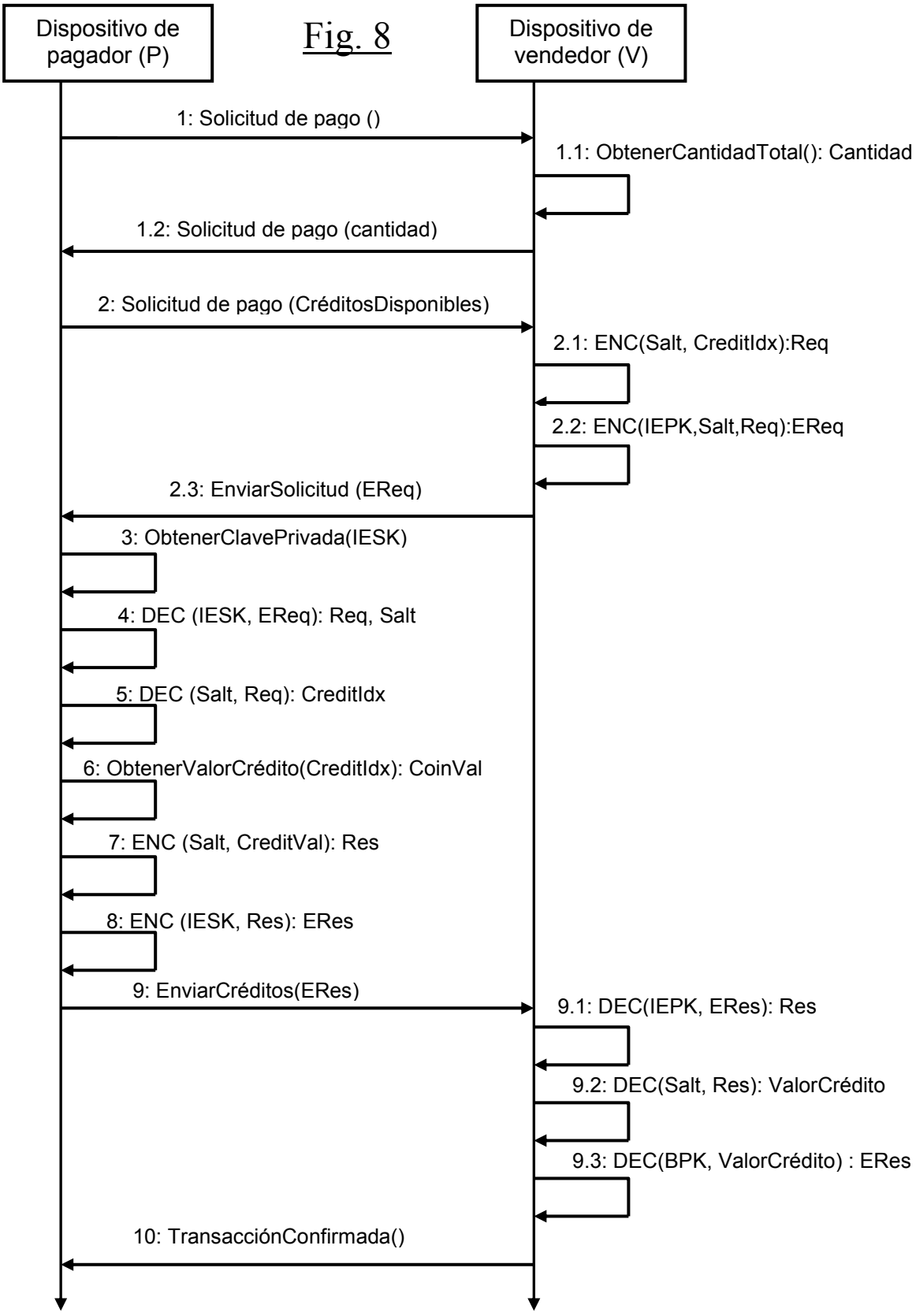
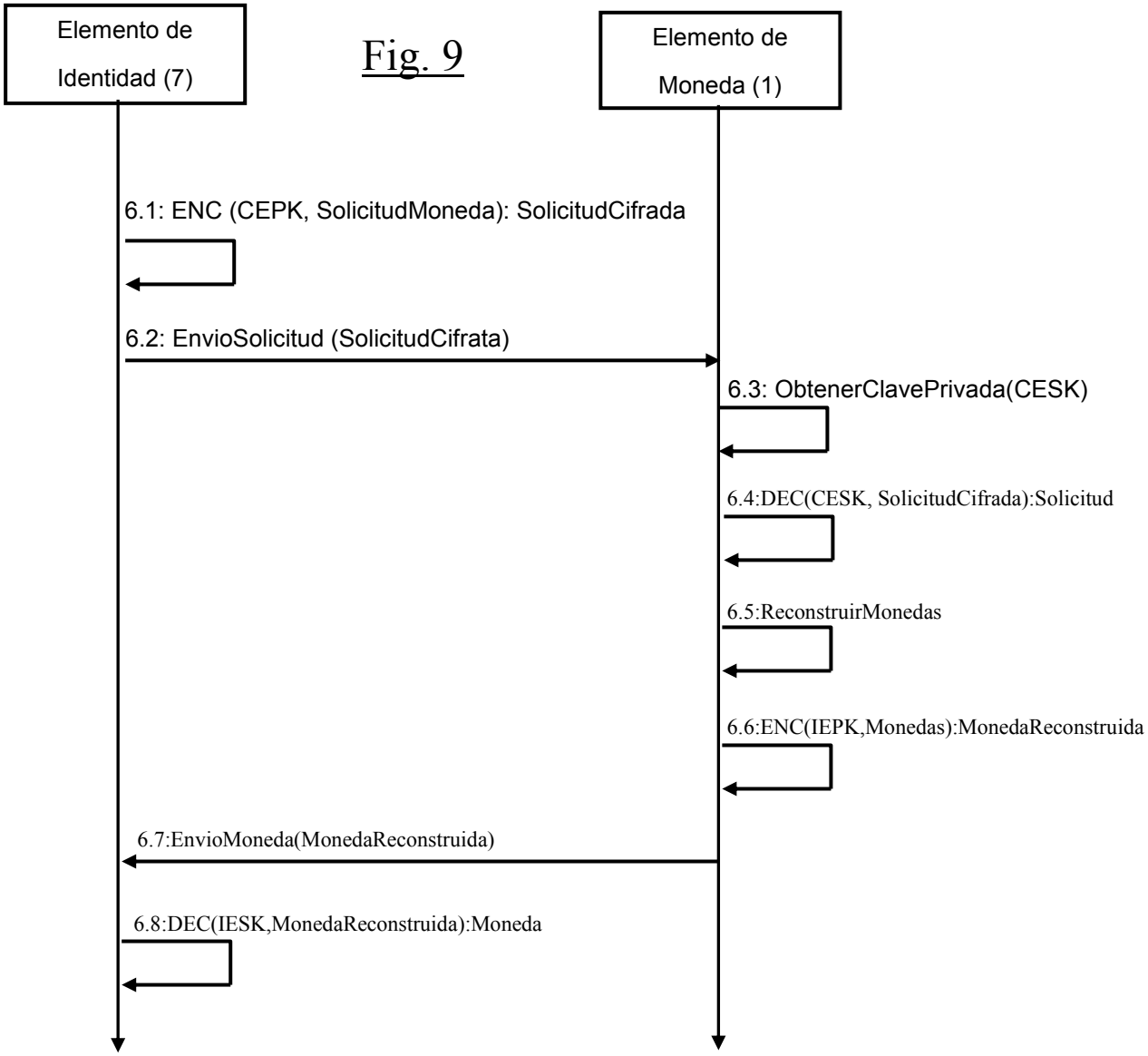

Dispositivo de pagador (P)
Dispositivo de vendedor (V)
1: Solicitud de pago ()
1.1: ObtenerCantidadTotal(): Cantidad
1.2: Solicitud de pago (cantidad)
2: Solicitud de pago (CréditosDisponibles)
2.1: ENC(Salt, CreditIdx):Req
2.2: ENC(IEPK,Salt,Req):EReq
2.3: EnviarSolicitud (EReq)
3: ObtenerClavePrivada(IESK)
4: DEC (IESK, EReq): Req, Salt
5: DEC (Salt, Req): CreditIdx
6: ObtenerValorCrédito(CreditIdx): CoinVal
7: ENC (Salt, CreditVal): Res
8: ENC (IESK, Res): ERes
9: EnviarCréditos(ERes)
9.1: DEC(IEPK, ERes): Res
9.2: DEC(Salt, Res): ValorCrédito
9.3: DEC(BPK, ValorCrédito) : ERes
10: TransacciónConfirmada()

Fig. 9


Elemento de Identidad (7)
Elemento de Moneda (1)
6.1: ENC (CEPK, SolicitudMoneda): SolicitudCifrada
6.2: EnvioSolicitud (SolicitudCifrata)
6.3: ObtenerClavePrivada(CESK)
6.4:DEC(CESK, SolicitudCifrada):Solicitud
6.5:ReconstruirMonedas
6.6:ENC(IEPK,Monedas):MonedaReconstruida
6.7:EnvioMoneda(MonedaReconstruida)
6.8:DEC(IESK,MonedaReconstruida):Moneda

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201431175

(22) Fecha de presentación de la solicitud: 01.08.2014

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06Q20/32*** (2012.01)
H04L9/00 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
Y	WO 2012122994 A1 (KREFT HEINZ) 20.09.2012, descripción: página 9, líneas 16-27; reivindicaciones 54-55.	1-5
Y	DE 102010045580 A1 (INFINEON TECHNOLOGIES AG) 22.03.2012, descripción: párrafos 14-16	1-5
A	KARNOUSKOS S Mobile payment: A journey through existing procedures and standardization initiatives. IEEE Communications Surveys and Tutorials, 20041001 Institute of Electrical and Electronics Engineers, US 01.10.2004 VOL: 2 No: 4 Págs: 44-66 ISSN 1553-877X. Todo el documento.	1,4
A	LING ZHANG et al. A Novel Off-line Anonymous and Divisible Digital Cash Protocol Utilizing Smart Card for Mobile Payment. Communications and Networking in China, 2006. ChinaCom '06. First International Conference on, 20061001 IEEE, Pi 01.10.2006 VOL: Págs: 1-6 ISBN 978-1-4244-0462-9; ISBN 1-4244-0462-2 Liang Shan; Linzhen Xie; Zhengbin Li; Anshi Xu. Todo el documento.	1,4
A	LIU WEN-YUAN et al. An Off-Line Divisible E-Cash Scheme Based on Smart Card.Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, 20070701 IEEE, Piscataway, NJ, USA 01.07.2007 VOL: Págs: 799-804 ISBN 978-0-7695-2909-7; ISBN 0-7695-2909-7 Chalabine M; Kessler C. Todo el documento.	1,4
A	LEKKAS et al. Implementing regular cash with blind fixed-value electronic coins. COMPUTER STANDARDS AND INTERFACES, 20070202 ELSEVIER SEQUOIA. LAUSANNE, CH 02.02.2007 VOL: 29 No: 3 Págs: 277-288 ISSN 0920-5489 Doi: doi:10.1016/j.csi.2006.01.005. Todo el documento.	1,4

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
30.10.2015	M. Muñoz Sánchez	1/5

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L, G06Q

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, XPIEE, XPI3E, NPL

Fecha de Realización de la Opinión Escrita: 30.10.2015

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-5	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-5	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	WO 2012122994 A1 (KREFT HEINZ)	20.09.2012
D02	DE 102010045580 A1 (INFINEON TECHNOLOGIES AG)	22.03.2012
D03	KARNOUSKOS S Mobile payment: A journey through existing procedures and standardization initiatives. IEEE Communications Surveys and Tutorials, 20041001 Institute of Electrical and Electronics Engineers, US 01.10.2004 VOL: 2 No: 4 Págs: 44-66 ISSN 1553-877X. Todo el documento.	01.10.2004
D04	LING ZHANG et al. A Novel Off-line Anonymous and Divisible Digital Cash Protocol Utilizing Smart Card for Mobile Payment.Communications and Networking in China, 2006. ChinaCom '06. First International Conference on, 20061001 IEEE, Pi 01.10.2006 VOL: Págs: 1-6 ISBN 978-1-4244-0462-9; ISBN 1-4244-0462-2 Liang Shan; Linzhen Xie; Zhengbin Li; Anshi Xu. Todo el documento.	01.10.2006
D05	LIU WEN-YUAN et al. An Off-Line Divisible E-Cash Scheme Based on Smart Card.Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, 20070701 IEEE, Piscataway, NJ, USA 01.07.2007 VOL: Págs: 799-804 ISBN 978-0-7695-2909-7; ISBN 0-7695-2909-7 Chalabine M; Kessler C. Todo el documento.	01.07.2007
D06	LEKKAS et al. Implementing regular cash with blind fixed-value electronic coins. COMPUTER STANDARDS AND INTERFACES, 20070202 ELSEVIER SEQUOIA. LAUSANNE, CH 02.02.2007 VOL: 29 No: 3 Págs: 277-288 ISSN 0920-5489 Doi: 10.1016/j.csi.2006.01.005. Todo el documento.	02.02.2007

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: El documento D01, divulga un método y dispositivos para la transferencia de dinero electrónico offline a través de un enlace entre pares. (p2p) en transacciones hechas en un punto de venta o entre usuarios. Una de las variantes del método consiste en utilizar una función física no clonable para añadir seguridad al módulo de hardware protegido contra su uso fraudulento: (**pág. 9, líneas 16-27**; "*Another possible way to use the hardware PUF for securing the tamper-protected hardware module is its use in a segmentation process of secrets (e.g. electronic tokens, encryption keys such as for example a secret key, a private key as part of a public key-pair, certificates, etc.) performed by the tamper-protected hardware module: A secret is split into two parts using a so called "constructor function" or "key generation function").*

El proceso consiste en la segmentación de secretos (tokens, claves privada-pública etc.). Los secretos se extraen del dispositivo usando la función constructora. Los secretos una vez utilizados pueden eliminarse de las memorias o registros internos. El módulo de hardware protegido contra su uso fraudulento genera una clave para cifrado/ descifrado de datos sobre la marcha y también para su identificación *(***Reivindicación 54***. A tamper-protected hardware module, comprising: a key generation unit adapted to autonomously generate in response to an initialization request a predetermined set of one or more symmetric keys and one or more asymmetric key pairs, one of the generated keys is used for identification of the tamper-protected hardware module, and an I/O-interface for providing, in response to the initialization request, the key used for identification of the tamper-protected hardware module to the outside of the tamper- protected hardware module and for receiving a certificate from a root certification authority comprising the key used for identification of the tamper-protected hardware module, a storage unit for storing the certificate comprising the key used for identification of the tamper-protected hardware module and the generated predetermined set of symmetric keys and asymmetric key pairs*.
Reivindicación 55*. The tamper-protected hardware module according to claim 54, wherein the key generation unit is adapted to generate a symmetric key for on-the-fly encryption/decryption of data to be maintained and/or stored inside or outside the tamper- protected hardware module in a host device including the tamper-protected hardware module prior to its exchange through the I/O-interface*).

A pesar de que el módulo de hardware del documento D01 genere sus propias claves de identificación y cifrado/ descifrado no incluye la separación y encadenamiento explícitas de las operaciones de cifrado y descifrado del proceso de transacciones monetarias en un punto de venta ni tampoco las solicitud de transacción del terminal del punto de venta que sí aparecen en la reivindicación 1. Sin embargo también incluiría implícitamente el selector de moneda. La diferencia mencionada supone a efectos técnicos la partición de la información sensible utilizando dos funciones físicas no clonables borrables en lugar de sólo una. El problema técnico objetivo sería así como conseguir esta doble seguridad.

Por su parte el documento D02 utiliza una PUF para generar una primera clave de cifrado/ descifrado y un generador de claves para obtener una segunda clave aleatoria, pudiendo usarse encadenadamente ambas para el cifrado/ descifrado de los datos: (**pár. 14-16;** "…*ferner eine Schlüsselerzeugungseinrichtung auf, wobei die Schlüsselerzeugungseinrichtung eingerichtet ist, um einen zweiten Schlüssel, mittels einer Zufallszah … Durch die Verwendung von zwei unterschiedlich erzeugten Schlüsseln zur Verschlüsselung, wird die Qualität/Stärke der Verschlüsselung der Datenwerte signifikant erhöht ... Der zweite Schlüssel kann beispielsweise unter Verwendung einer Zufallszahl erzeugt werden, wobei die Zufallszahl beispielsweise durch einen Random Number Generators (RNG) generiert werden kann… Der erste und der zweite Schlüssel können entweder zu einem gemeinsamen Schlüssel zusammengelegt werden oder es finden zwei voneinander getrennte Verschlüsselungen des Datenwertes mittels einer oder zwei kryptographischer Einheiten statt. Eine der kryptographischen Einheiten kann dabei beispielsweise eine so genannte Memory Encryption Decryption Unit (MED) sein."*)
Teniendo en cuenta la complementariedad de ambos documentos y las posibilidades sugeridas en ellos el experto en la materia se vería orientado a añadir una segunda PUF en combinación o aparte del generador de números aleatorios en las operaciones de cifrado/ descifrado para garantizar una mayor seguridad en las transacciones monetarias.
Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley de Patentes.

Reivindicación 4: el procedimiento reivindicado se corresponde directamente con las operaciones que realizarían los elementos funcionales del dispositivo de la reivindicación 1, por lo que del análisis de esta se concluye igualmente que la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 4 según el art. 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2, 3 y 5: las particularidades incluidas en estas reivindicaciones ya se han discutido en el análisis de la reivindicación 1 por lo que de lo dicho respecto a aquella se concluye que la combinación de los documentos D01 y D02 también afecta a la actividad inventiva de las reivindicaciones 2, 3 y 5 según el art. 8.1 de la Ley de Patentes.