(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 978 986**

(51) Int. Cl.:

H04W 12/71 (2011.01)
H04W 12/72 (2011.01)
G06F 21/32 (2013.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.04.2013 E 13162498 (3)**

(97) Fecha y número de publicación de la concesión europea: **03.04.2024 EP 2657876**

(54) Título: **Circuito de verificación de identidad real y virtual, sistema del mismo y método de transacción electrónica**

(30) Prioridad:

25.04.2012 TW 101114614

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.09.2024

(73) Titular/es:

SAMTON INTERNATIONAL DEVELOPMENT TECHNOLOGY CO., LTD. (100.0%)
Offshore Chambers, P.O. Box 217
APIA, WS

(72) Inventor/es:

SUNG, CHIA-YU;
JIAN, YU-CHUAN;
JIAN, YU-CHANG y
TSUI, YI FEN

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Circuito de verificación de identidad real y virtual, sistema del mismo y método de transacción electrónica

Campo de la invención

Esta invención se refiere a un circuito de verificación de identidad real y virtual, un sistema que comprende el mismo y un método de transacción electrónica, capaz de realizar verificación de identidad electrónica con alta seguridad en un entorno virtual en internet mediante el uso de la característica biológica única de un usuario en un entorno real.

Descripción de la técnica relacionada

Recientemente, con la creciente popularidad del entorno virtual establecido por internet y su penetración en el entorno real de los consumidores, aparecen rápidamente nuevos estilos de vida que cambian los hábitos de consumo de las personas. Por ejemplo, en lugar de realizar compras en una tienda real, cada vez más consumidores optan por realizar transacciones en línea en un entorno virtual, tal como una plataforma de compras creada en internet.

Hay varias razones por las que las tiendas virtuales reemplazan gradualmente a las reales y captan una parte sustancial del mercado. A diferencia de las tiendas reales, el entorno virtual proporciona un canal de ventas de bajo coste para reducir considerablemente los costes reales de las tiendas y los costes de personal. Además, el entorno virtual proporciona a los consumidores mucha más flexibilidad, permitiéndoles realizar compras en cualquier momento y lugar.

Sin embargo, la cuestión más importante para el consumo en el entorno virtual es cómo determinar la identidad del consumidor en el entorno real. Al parecer, la identidad del consumidor puede confirmarse mediante un certificado de identidad real o una prueba de identidad; sin embargo, en el entorno virtual, los documentos son propensos a sufrir modificaciones ya que sólo están disponibles en formato electrónico. En consecuencia, es deseable verificar la identidad de un consumidor de una manera altamente segura en el entorno virtual.

Para abordar el problema identificado anteriormente, se han propuesto muchas soluciones. Por ejemplo, los consumidores pueden crear primero una cuenta que represente su identidad y un conjunto de contraseñas para la cuenta, de modo que puedan realizar operaciones en el entorno virtual con la cuenta y la contraseña, tal como realizar transacciones electrónicas con una tarjeta de crédito y la cuenta, así como la contraseña. Sin embargo, la seguridad puede verse comprometida si se piratea la cuenta y la contraseña o incluso la tarjeta de crédito. Otro enfoque es verificar electrónicamente un documento de identidad, que utilizan principalmente las agencias gubernamentales. Por ejemplo, una tarjeta IC de certificación se emite previa solicitud de una oficina de registro de hogares de acuerdo con la identidad única del solicitante, y la tarjeta IC de certificación puede utilizarse para representar la identidad del titular. Aunque el sistema de identidad electrónica establecido por el gobierno tiene autoridad y es confiable, el proceso de verificación aún puede verse dañado porque utiliza contraseñas fijas. Además, para mantener su seguridad, el sistema adopta un diseño cerrado limitado principalmente con propósitos gubernamentales y rara vez está abierto al sector privado.

Además, algunos productos, tales como los billetes de lotería, no son actualmente adecuados para el consumo mediante transacciones electrónicas. Los billetes de lotería son instrumentos de valor no inscritos, por lo que se considera propietario a quien posee un billete de lotería. Por lo tanto, la compra de billetes de lotería normalmente la deben realizar los consumidores en persona, lo que hace que la transacción de lotería sea bastante inconveniente.

El documento US20060016871A1 divulga un sistema y métodos para la seguridad biométrica que utilizan biometría de escaneo de pulsaciones de claves en un sistema lector de tarjetas inteligentes. El sistema de seguridad biométrico también incluye un sensor de escaneo de pulsaciones de claves que detecta muestras biométricas y un dispositivo para verificar muestras biométricas. En una realización, el sistema de seguridad biométrico incluye una tarjeta inteligente configurada con un sensor de escaneo de pulsaciones de claves. En otra realización, el sistema incluye un lector configurado con un sensor de escaneo de pulsaciones de claves. En otra realización más, la presente invención divulga métodos para ofrecer y procesar muestras de escaneo de pulsaciones de claves para facilitar la autorización de transacciones. La patente de Estados Unidos 5,280,527 divulga la generación de un autentificador de seguridad, mediante un aparato de seguridad biométrico, utilizando entrada biométrica junto con un código "fijo" secreto (es decir, PIN) y una "información autogenerada" pública y variable en el tiempo. El autentificador de seguridad resultante puede visualizarse al usuario para su entrada manual o transmitirse a un servidor principal que decodifica el autentificador para identificar el código fijo incorporado y autenticar al usuario para que se le permita realizar una transacción de transferencia de fondos. La "información de autogeneración variable en el tiempo" se genera mediante un generador de código variable en el tiempo que está integrado en el aparato de seguridad biométrico. La publicación de solicitud de patente de Estados Unidos US 2002/0144128 divulga que se puede generar una contraseña biométrica utilizando una combinación de datos biométricos de un usuario junto con una contraseña de un solo uso (OTP).

En consecuencia, la presente invención proporciona un circuito de verificación de identidad real y virtual, un sistema que comprende el mismo y un método de transacción electrónica para abordar los inconvenientes mencionados anteriormente.

Resumen de la invención

Un objeto de esta invención es proporcionar un circuito de verificación de identidad real y virtual capaz de incorporarse o conectarse con un dispositivo electrónico para llevar a cabo una verificación de identidad electrónica altamente segura de un usuario con su característica biológica única en un servidor remoto.

Es otro objeto de esta invención utilizar el circuito de verificación de identidad real y virtual antes mencionado, mediante la generación de un código de característica biológica asociado con la característica biológica única de un usuario mediante varios procesos de negociación, para lograr diversos tipos de verificación de identidad electrónica.

Otro objeto de esta invención es proporcionar un sistema de verificación de identidad real y virtual para la verificación de identidad electrónica, que está formado por el circuito de verificación de identidad real y virtual y el servidor.

Otro objeto más de esta invención es proporcionar un método de transacción electrónica que realice transacciones electrónicas altamente seguras en el entorno real a través del entorno virtual con base en el resultado de la verificación de identidad electrónica realizada por el sistema de verificación de identidad real y virtual.

Estos y otros objetos se logran mediante un circuito de verificación de identidad real y virtual capaz de incorporarse o conectarse con un dispositivo electrónico para permitir que un usuario lleve a cabo una verificación de identidad electrónica con su característica biológica única en un servidor que almacena datos asociados con la característica biológica. El circuito de verificación de identidad real y virtual comprende una unidad de memoria, una unidad de adquisición, una unidad de procesamiento y una unidad de comunicación. La unidad de memoria tiene un espacio de almacenamiento para almacenar un código de clave de verificación. La unidad de adquisición adquiere la característica biológica y genera un código de característica biológica correspondiente. La unidad de procesamiento, que está conectada con la unidad de memoria y la unidad de adquisición y provista de un proceso de negociación, procesa el código de clave de verificación y el código de característica biológica de acuerdo con el proceso de negociación para generar un código no verificado correspondiente. La unidad de comunicación, que está conectada con la unidad de procesamiento, transmite el código no verificado a internet y espera un resultado de la verificación de identidad electrónica asociada con el código no verificado desde el servidor.

Estos y otros objetos también se logran mediante un sistema de verificación de identidad real y virtual que permite al usuario realizar una verificación de identidad electrónica con su característica biológica única. El sistema comprende un dispositivo electrónico y un servidor. El dispositivo electrónico comprende una unidad de memoria, una unidad de adquisición, una unidad de procesamiento y una unidad de comunicación, en donde la unidad de memoria tiene un espacio de almacenamiento para almacenar un código clave de verificación; la unidad de adquisición adquiere la característica biológica y genera un código de característica biológica correspondiente a la característica biológica; la unidad de procesamiento está conectada con la unidad de memoria y la unidad de adquisición y se le proporciona un proceso de negociación, procesando la unidad de procesamiento el código de clave de verificación y el código de característica biológica de acuerdo con el proceso de negociación para generar un código no verificado correspondiente; y la unidad de comunicación se conecta con la unidad de procesamiento y transmite el código no verificado a internet. El servidor comprende una unidad de base de datos, una unidad transceptora, una unidad de verificación y una unidad de retroalimentación, en donde la unidad de base de datos almacena la característica biológica del usuario; la unidad transceptora recibe el código no verificado; la unidad de verificación está conectada con la unidad de base de datos y la unidad transceptora y adaptada para verificar la característica biológica y el código no verificado para generar un resultado de verificación; y la unidad de retroalimentación está conectada con la unidad de verificación y adaptada para enviar el resultado de la verificación al dispositivo electrónico a través de la unidad transceptora para completar la verificación de la identidad del usuario.

Estos y otros objetos se logran además mediante un método de transacción electrónica que permite a un usuario realizar una transacción electrónica en al menos un subservidor de transacciones conectado con un servidor de transacciones que contiene un trayecto de enlace indicado del subservidor de transacciones después de que el usuario obtiene un resultado de verificación de identidad electrónica realizada mediante un sistema de verificación de identidad real y virtual que incluye un dispositivo electrónico y un servidor con el uso de una característica biológica, el método que comprende (a) conectar el dispositivo electrónico al servidor de transacciones para seleccionar el trayecto de enlace indicado del subservidor de transacciones en el servidor de transacciones; y (b) utilizar el dispositivo electrónico para recibir el resultado de la verificación de manera que el servidor de transacciones permita selectivamente al usuario realizar la transacción electrónica, en donde el usuario está habilitado selectivamente para realizar la transacción electrónica en el subservidor de transacciones directamente a través del servidor de transacciones de acuerdo con el resultado de la verificación y el trayecto de enlace indicado.

En una realización, la transacción electrónica está relacionada con la lotería electrónica, el servidor de transacciones es una plataforma financiera y el subservidor de transacciones es una máquina expendedora de lotería.

A diferencia de las técnicas anteriores, el circuito de verificación de identidad real y virtual, el sistema del mismo y el método de transacción electrónica permiten a un usuario convertir su característica biológica en un código de característica biológica correspondiente con el uso de uno de una pluralidad de procesos de negociación, y el código de característica biológica puede ser utilizado por un servidor remoto para realizar la verificación electrónica de la

identidad del usuario. En un aspecto, el servidor es capaz de confirmar la coherencia entre el código de característica biológica y la característica biológica almacenada en el servidor, y el resultado de la verificación luego se transmite de regreso al circuito de verificación de identidad real y virtual para completar la verificación de identidad electrónica del usuario. En consecuencia, el usuario puede realizar transacciones electrónicas altamente seguras de acuerdo con el resultado de la verificación, tal como comprar un billete de lotería electrónico en un modo de transacción de lotería.

Breve descripción de los dibujos

Se puede obtener una comprensión más completa del tema en cuestión haciendo referencia a la descripción detallada y las reivindicaciones cuando se consideran junto con las siguientes figuras, en donde números de referencia similares se refieren a elementos similares en todas las figuras.

La figura 1 ilustra un diagrama de bloques del circuito de verificación de identidad real y virtual de una realización de esta invención;

La figura 2 ilustra un diagrama de bloques del sistema de verificación de identidad real y virtual de una realización de esta invención;

La figura 3 ilustra un diagrama de bloques del método de transacción electrónica de una realización de esta invención; y

La figura 4 ilustra un diagrama de flujo del método de transacción electrónica de la figura 3.

Descripción de realizaciones

En las figuras adjuntas se ilustran realizaciones para mejorar la comprensión de los conceptos, características y ventajas presentadas por la presente invención.

La figura 1 ilustra un diagrama de bloques del circuito de verificación de identidad real y virtual de una realización de esta invención. El circuito 10 de verificación de identidad real y virtual permite a un usuario 2 realizar una verificación de identidad electrónica con su característica biológica BC única en un servidor 6, almacenando previamente los datos asociados con la característica biológica BC en internet 4. En una realización, la característica biológica BC puede ser, por ejemplo, una huella dactilar, un patrón de iris, una huella de palma, un patrón de venas, un patrón de sonido o un patrón facial del usuario 2.

El circuito 10 de verificación de identidad real y virtual puede estar incorporado o conectado con un dispositivo 8 electrónico. En otras palabras, el circuito 10 de verificación de identidad real y virtual puede estar integrado en un dispositivo 8 electrónico o conectado con un dispositivo 8 electrónico externo. El dispositivo 8 electrónico puede ser un dispositivo de comunicación móvil portátil, una tableta o un ordenador personal fijo. Si el circuito 10 de verificación de identidad real y virtual se utiliza externamente desde el dispositivo 8 electrónico, puede integrarse en otro producto electrónico tal como una unidad flash.

En una realización, el circuito 10 de verificación de identidad real y virtual comprende una unidad 12 de memoria, una unidad 14 de adquisición, una unidad 16 de procesamiento y una unidad 18 de comunicación.

La unidad 12 de memoria tiene un espacio de almacenamiento para almacenar un código de clave de verificación VKC, que se genera mediante uno cualquiera de los siguientes procedimientos:

1) el código de clave de verificación VKC correspondiente a la característica biológica BC se guarda previamente en la unidad 12 de memoria;

2) la unidad 12 de memoria está provista del código de clave de verificación VKC que está asociado con el dispositivo 8 electrónico, tal como una de una dirección de control de acceso a medios (MAC), un módulo de identidad de suscriptor (SIM) y una contraseña del dispositivo 8 electrónico que el usuario puede establecer de forma flexible;

3) la unidad 12 de memoria recibe a través de la unidad 18 de comunicación un código de clave variable VKC' generado por un servidor de terceros o el servidor 6 y forma el código de clave de verificación VKC, de manera que el código de clave variable VKC' permita el cambio periódico del código de clave de verificación VKC. Por ejemplo, el código de clave variable VKC' se cambia pasivamente dentro de una duración tal como microsegundos, milisegundos, segundos, horas, días, meses o años. Alternativamente, en un modo de reemplazo activo, el circuito 10 de verificación de identidad real y virtual puede recuperar el código de clave variable VKC' del servidor de terceros o del servidor 6 sólo cuando el usuario 2 procede a la verificación de identidad electrónica; y

4) el código de clave de verificación VKC se forma a partir de la característica biológica BC obtenida por la unidad 14 de adquisición y se guarda en la unidad 12 de memoria. Como tal, al usuario 2 se le permite establecer de manera flexible el código de clave de verificación VKC asociado con la característica biológica BC con el propósito de verificar la identidad electrónica.

La unidad 14 de adquisición está configurada para adquirir la característica biológica BC y generar un código de característica biológica BCC correspondiente a la característica biológica BC. En una realización, la unidad 14 de adquisición, tal como una cámara o un dispositivo de reconocimiento de huellas dactilares, está configurada para adquirir, entre otros, una huella dactilar, un patrón de iris, una huella de la palma, un patrón de venas, un patrón de sonido o un patrón facial.

La unidad 16 de procesamiento está conectada con la unidad 12 de memoria y la unidad 14 de adquisición y está provista de un proceso de negociación DP, de manera que la unidad 16 de procesamiento procesa el código de clave de verificación VKC y el código de característica biológica BCC para generar un código no verificado correspondiente UVC. En una realización, el proceso de negociación DP está configurado para uno cualquiera de los siguientes propósitos:

1) el proceso de negociación DP compara el código de característica biológica BCC con el código de clave de verificación VKC para determinar si se genera el código no verificado UVC;

2) el proceso de negociación DP codifica el código de característica biológica BCC y el código de clave de verificación VKC para generar el código no verificado UVC que corresponde o incluye el código de característica biológica BCC y el código de clave de verificación VKC; y

3) el proceso de negociación DP selecciona el código de característica biológica BCC o el código de clave de verificación VKC para generar el código no verificado UVC.

La unidad 18 de comunicación está conectada con la unidad 16 de procesamiento para transmitir el código no verificado UVC a internet 4 y esperar un resultado de verificación VR de la verificación de identidad electrónica asociada con el código no verificado UVC desde el servidor 6. En una realización, la unidad 18 de comunicación transmite el código no verificado UVC mediante comunicación alámbrica o inalámbrica, y la unidad 18 de comunicación cumple con un protocolo de comunicación de Bluetooth, comunicación de red fija, comunicación móvil o WI-FI.

La figura 2 ilustra un diagrama de bloques del sistema de verificación de identidad real y virtual de una realización de esta invención. El sistema 20 de verificación de identidad real y virtual permite al usuario 2 llevar a cabo una verificación de identidad electrónica con su característica biológica BC única. En esta realización, el sistema 20 de verificación de identidad real y virtual comprende un dispositivo 22 electrónico y un servidor 24.

Como se mencionó en la realización anterior, el dispositivo 22 electrónico está incorporado con el circuito 10 de verificación de identidad real y virtual que comprende la unidad 12 de memoria, la unidad 14 de adquisición, la unidad 16 de procesamiento y la unidad 18 de comunicación.

El servidor 24 comprende una unidad 242 de base de datos, una unidad 244 transceptora, una unidad 246 de verificación y una unidad 248 de retroalimentación.

La unidad 242 de base de datos está configurada para almacenar la característica biológica BC del usuario 2, que puede adquirirse por adelantado y guardarse en la unidad 242 de base de datos para completar el registro de la característica biológica BC en la misma. En una realización, la unidad 242 de base de datos está configurada para almacenar la característica biológica BC como una huella dactilar, un patrón de iris, una huella de palma, un patrón de venas, un patrón de sonido o un patrón facial.

La unidad 244 transceptora está configurada para recibir el código no verificado UVC.

La unidad 246 de verificación está conectada con la unidad 242 de base de datos y la unidad 244 transceptora y configurada para verificar, tal como por comparación, la característica biológica BC y el código no verificado UVC y determinar si el código no verificado UVC coincide con la característica biológica BC guardada previamente en la unidad 242 de base de datos para generar el resultado de la verificación VR que indica el resultado de la verificación, tal como coincidente, no coincidente o fallo de determinación.

La unidad 248 de retroalimentación está conectada con la unidad 246 de verificación y configurada para enviar el resultado de la verificación VR al dispositivo 22 electrónico para completar la verificación de la identidad del usuario.

Las figuras 3 y 4 ilustran respectivamente un diagrama de bloques y un diagrama de flujo del método de transacción electrónica de una realización de esta invención. En la ilustración de arquitectura de la figura 3, el método de transacción electrónica permite al usuario 2 realizar una transacción electrónica en al menos un subservidor 28 de transacciones (por ejemplo, un sitio web de compras o una máquina expendedora de lotería) conectado con un servidor 26 de transacciones (por ejemplo, un servidor bancario o una plataforma de flujo de efectivo) que contiene un trayecto de enlace indicado ILP del subservidor 28 de transacciones después de que el usuario 2 obtiene un resultado de verificación VR de verificación de identidad electrónica realizada por un sistema de verificación de identidad real y virtual que incluye el dispositivo 8 electrónico y el servidor 24 con el uso de una característica biológica.

En la figura 4, el método de transacción electrónica comienza con el paso S41 para conectar el dispositivo 8 electrónico al servidor 26 de transacciones para seleccionar el trayecto de enlace indicado ILP del subservidor 28 de transacciones en el servidor 26 de transacciones.

A continuación, el paso S42 comprende utilizar el dispositivo 8 electrónico para recibir el resultado de verificación VR del usuario 2 de manera que el servidor 26 de transacciones permita selectivamente al usuario 2 realizar la transacción electrónica, mediante el cual se habilita selectivamente al usuario 2 para realizar la transacción electrónica en el subservidor 28 de transacciones directamente a través del servidor 26 de transacciones de acuerdo con el resultado de la verificación VR y el trayecto de enlace indicado ILP.

En una realización, el servidor 26 de transacciones proporciona al dispositivo 8 electrónico la ubicación geográfica de un subservidor 28 de transacciones en proximidad al dispositivo 8 electrónico de acuerdo con una de la ubicación geográfica del dispositivo 8 electrónico y la información relacionada con el usuario 2.

En otra realización, la transacción electrónica está relacionada con la lotería electrónica, el servidor 26 de transacciones es una plataforma financiera y el subservidor 28 de transacciones es una máquina expendedora de lotería.

En el modo de transacción electrónica de lotería electrónica, después de que el usuario 2 realiza la transacción electrónica en la máquina expendedora de lotería, la máquina expendedora de lotería produce un billete de lotería en papel que contiene información de la lotería, tal como el número elegido por el usuario 2.

Además, la información de lotería del billete de lotería en papel se transmite entonces de nuevo al dispositivo 8 electrónico para permitir únicamente que el usuario 2 con la característica biológica BC posea virtualmente el billete de lotería en papel.

En otra realización, el subservidor 28 de transacciones conserva el billete de lotería en papel y asocia la característica biológica BC del usuario 2 con el billete de lotería en papel para permitir únicamente al usuario 2 con la característica biológica BC adquirir el billete de lotería en papel.

Además, al usuario 2 se le permite recuperar el billete de lotería en papel de la máquina expendedora de lotería con la característica biológica BC.

El circuito de verificación de identidad real y virtual, su sistema y el método de transacción electrónica permiten a un usuario convertir su característica biológica en un código de característica biológica correspondiente con el uso de uno de una pluralidad de procesos de negociación, y el código de característica biológica puede ser utilizado por un servidor remoto para realizar la verificación electrónica de la identidad del usuario. En un aspecto, el servidor es capaz de confirmar la coherencia entre el código de característica biológica y la característica biológica almacenada en el servidor, y el resultado de la verificación luego se transmite de regreso al circuito de verificación de identidad real y virtual para completar la verificación de identidad electrónica del usuario. En consecuencia, el usuario puede realizar transacciones electrónicas altamente seguras de acuerdo con el resultado de la verificación, tal como comprar un billete de lotería electrónico en un modo de transacción de lotería.

Si bien estas descripciones describen directamente las realizaciones anteriores, se entiende que los expertos en la técnica pueden concebir modificaciones y/o variaciones a las realizaciones específicas mostradas y descritas en este documento. Sin embargo, cualquier modificación o variación que caiga dentro del alcance de esta descripción también debe incluirse en la misma.

REIVINDICACIONES

1. Un sistema de verificación de identidad real y virtual que permite a un usuario realizar una verificación de identidad electrónica con su característica biológica (BC) única para hacer una transacción electrónica en un servidor (26) de transacciones, que comprende:

un dispositivo (22) electrónico que comprende:

una unidad (12) de memoria que tiene un espacio de almacenamiento para almacenar un código de clave de verificación (VKC) y un código de clave variable (VKC'), en donde el código de clave variable (VKC') se cambia pasivamente dentro de un período y se genera por un servidor de terceros o un servidor (24), y la unidad (12) de memoria también está adaptada para almacenar previamente el código de clave de verificación (VKC) asociado a la característica biológica (BC);

una unidad (14) de adquisición para adquirir la característica biológica (BC) y generar un código de característica biológica (BCC) correspondiente a la característica biológica;

caracterizado porque una unidad (16) de procesamiento está conectada con la unidad (12) de memoria y la unidad (14) de adquisición y está provista de un proceso de negociación (DP) que compara el código de característica biológica (BCC) con el código de clave de verificación (VKC) para determinar si se debe generar un código no verificado (UVC) al principio y cuando el código de característica biológica (BCC) coincide con el código de clave de verificación (VKC), la unidad (16) de procesamiento procesa adicionalmente el código de clave variable (VKC') y el código de característica biológica (BCC) de acuerdo con el proceso de negociación (DP) para generar un código no verificado correspondiente (UVC), en donde el código no verificado (UVC) está relacionado con el código de característica biológica (BCC) y el código de clave variable (VKC'), el código de característica biológica (BCC) es variable mediante el cálculo con el código de clave variable (VKC') para hacer que el código no verificado (UVC) tenga el código de característica biológica (BCC) variable, y el proceso de negociación (DP) está configurado para realizar al menos uno de:

(a) codificar el código de característica biológica (BCC) y el código de clave variable (VKC') para generar el código no verificado (UVC) correspondiente al código de característica biológica (BCC) y el código de clave variable (VKC'); y

(b) seleccionar uno del código de característica biológica (BCC) y el código de clave variable (VKC') para generar el código no verificado (UVC); y

una unidad (18) de comunicación conectada con la unidad (16) de procesamiento y que transmite el código no verificado (UVC) a internet, en donde la unidad (18) de comunicación recibe el código de clave variable (VKC') a la unidad (12) de memoria; y

el servidor (24) que comprende:

una unidad (242) de base de datos para almacenar la característica biológica (BC) del usuario;

una unidad (244) transceptora para recibir el código no verificado (UVC) y enviar el código de clave variable (VKC') y un resultado de verificación (VR) al dispositivo (22) electrónico;

una unidad (246) de verificación conectada con la unidad (242) de base de datos y la unidad (244) transceptora y verificando la característica biológica (BC) y el código no verificado (UVC) para generar el resultado de verificación (VR); y

una unidad (248) de retroalimentación conectada con la unidad (246) de verificación y la unidad (244) transceptora;

en donde el dispositivo (22) electrónico recibe el resultado de la verificación (VR) y utiliza el resultado de la verificación (VR) para lograr la verificación de la identidad del usuario que realiza la transacción electrónica en un servidor (26) de transacciones.

2. El sistema de verificación de identidad real y virtual de la reivindicación 1, en donde el código de clave de verificación (VKC) se deriva de al menos uno de una dirección de control de acceso a medios, un módulo de identidad de suscriptor y una contraseña establecida por el usuario del dispositivo (22) electrónico.

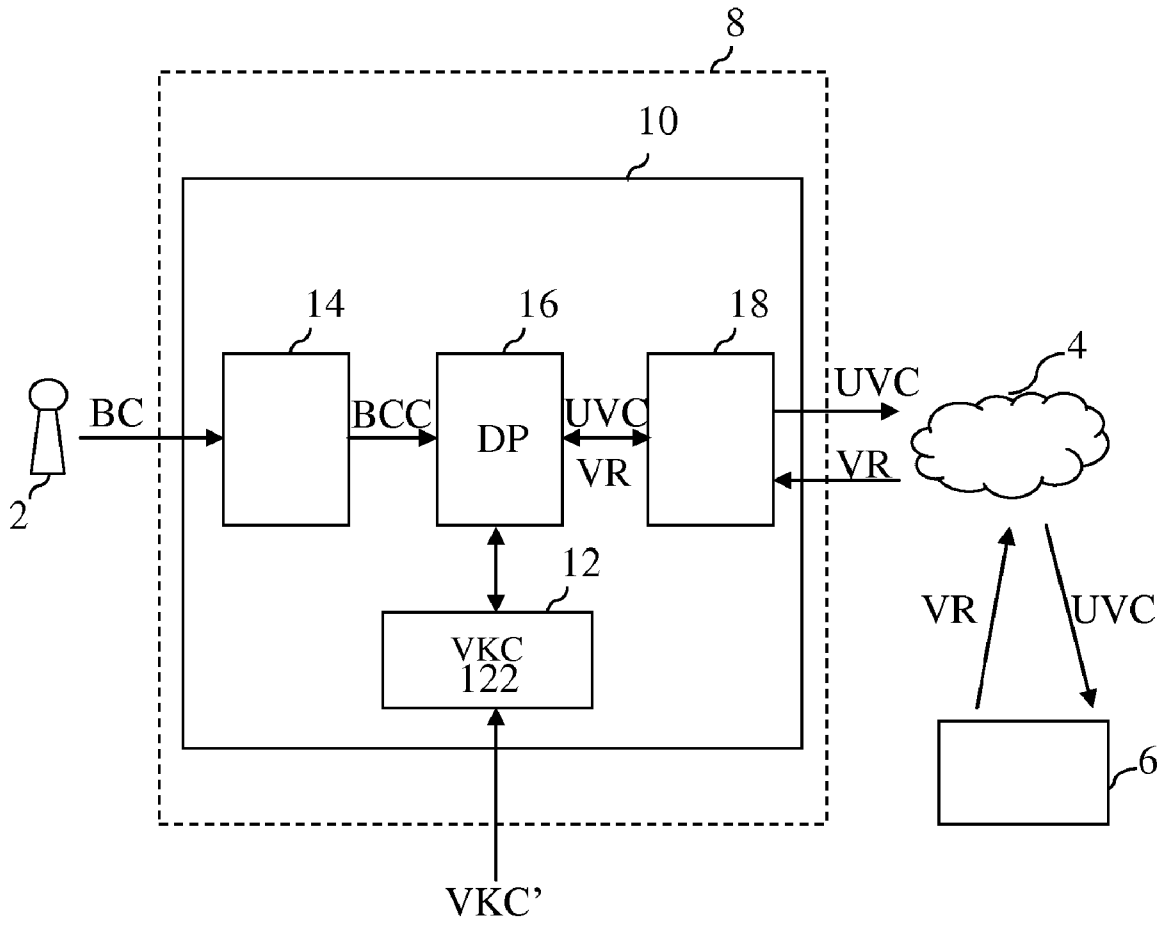

FIG. 1

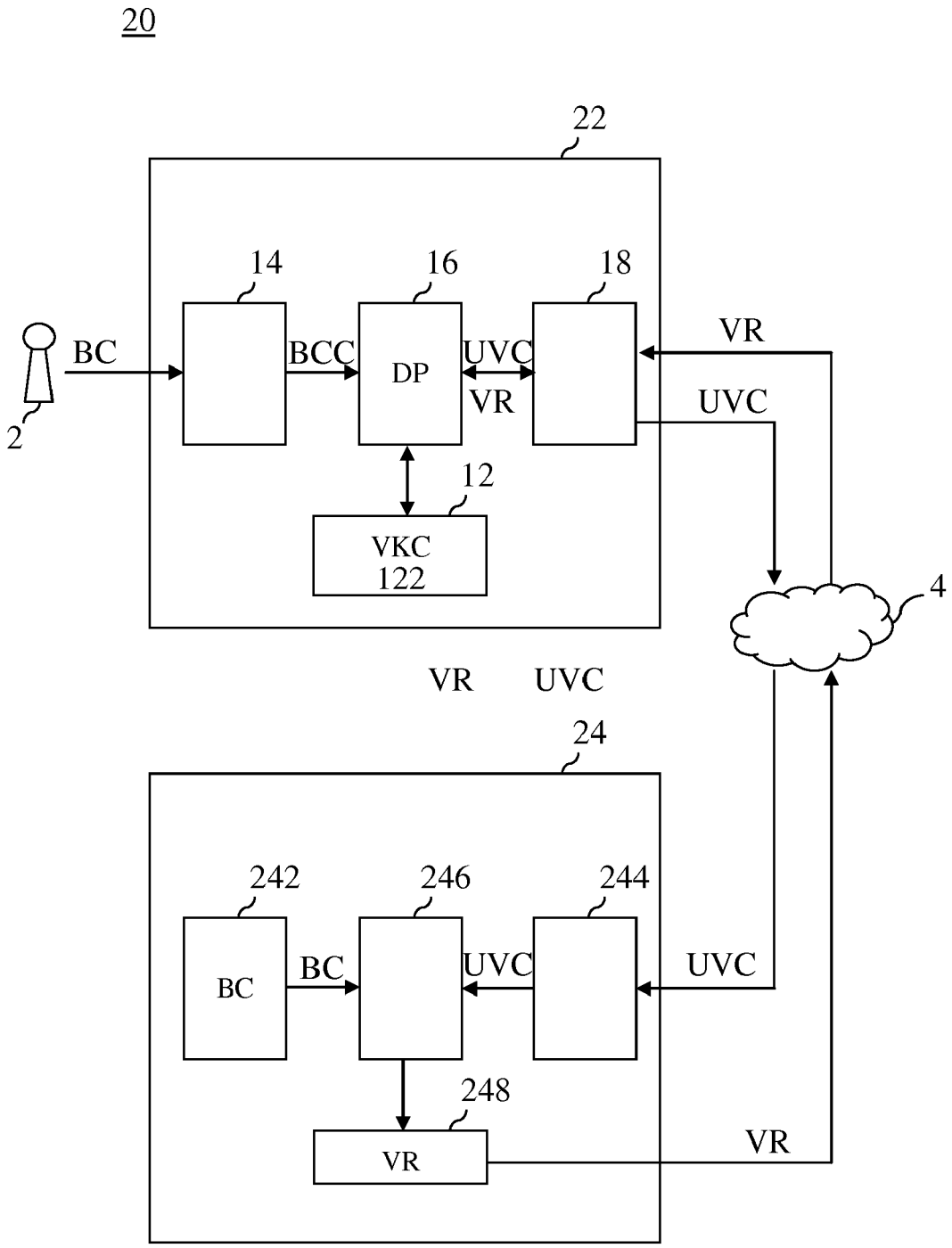
20
22
14
16
18
BC
BCC
DP
UVC
VR
VR
UVC
2
12
VKC
122
4
VR
UVC
24
242
246
244
BC
BC
UVC
UVC
248
VR
VR

FIG. 2

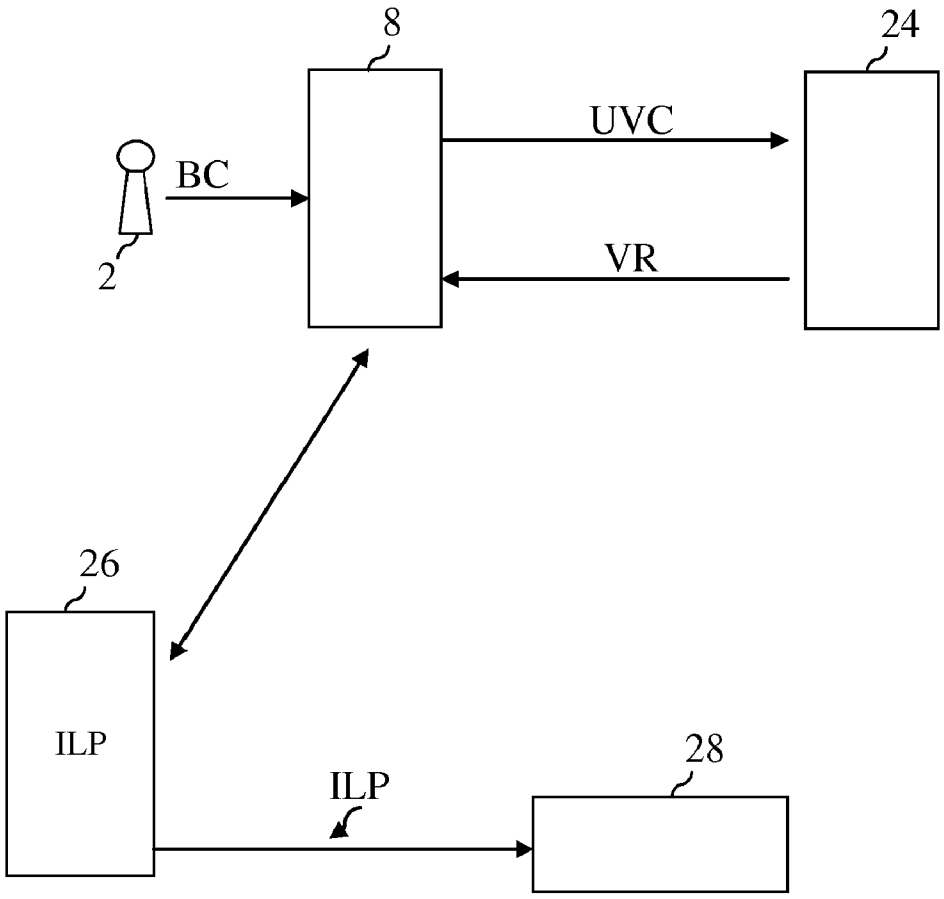

FIG. 3

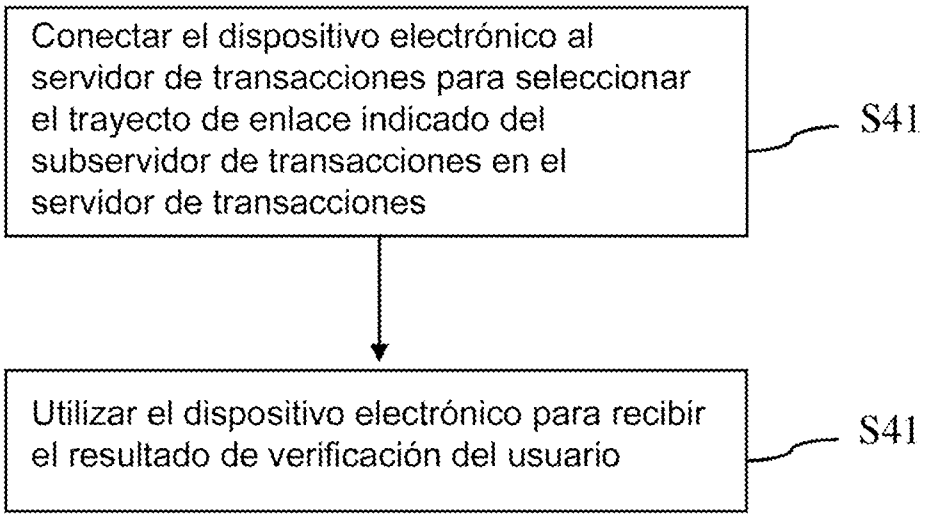
Conectar el dispositivo electrónico al servidor de transacciones para seleccionar el trayecto de enlace indicado del subservidor de transacciones en el servidor de transacciones
S41
Utilizar el dispositivo electrónico para recibir el resultado de verificación del usuario
S41

FIG. 4