

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 830 387**

51 Int. Cl.:

H04L 29/06 (2006.01)
H04B 5/00 (2006.01)
H04W 12/06 (2009.01)
H04W 4/80 (2008.01)
G06F 21/64 (2013.01)
G06Q 20/16 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **01.06.2015 PCT/US2015/033478**

87 Fecha y número de publicación internacional: **10.12.2015 WO15187533**

96 Fecha de presentación y número de la solicitud europea: **01.06.2015 E 15803610 (3)**

97 Fecha y número de publicación de la concesión europea: **12.08.2020 EP 3183701**

54 Título: **Cliente, plataforma informática, y procedimientos para llevar a cabo transacciones seguras**

30 Prioridad:

02.06.2014 US 201414293112

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

03.06.2021

73 Titular/es:

**CERTUS TECHNOLOGY SYSTEMS INC. (100.0%)
3450 Sacramento St. 327
San Francisco, CA 94118, US**

72 Inventor/es:

WOLOSEWICZ, JACK

74 Agente/Representante:

TORNER LASALLE, Elisabet

ES 2 830 387 T3

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

DESCRIPCIÓN

Cliente, plataforma informática, y procedimientos para llevar a cabo transacciones seguras

Solicitudes relacionadas

- 5 Esta es una solicitud PCT que reivindica prioridad a la solicitud de patente no provisional estadounidense nº 14/293,112 presentada el 2 de junio de 2014 titulada "CLIENT, COMPUTING PLATFORM, AND METHODS FOR CONDUCTING SECURE TRANSACTIONS".

Campo de la invención

La invención se refiere a plataformas cliente e informáticas que pueden ser usadas para llevar a cabo transacciones seguras.

10 Antecedentes de la invención

- 15 Dado que el comercio electrónico sigue ganando popularidad, a un usuario que puede adquirir una variedad de artículos de múltiples portales electrónicos, a veces, se le puede pedir que recuerde una contraseña particular para cada portal electrónico o vendedor con el que hace negocios el usuario. En algunos casos, un usuario puede hacer uso de una contraseña idéntica para múltiples portales electrónicos, de forma que reduzca la necesidad del usuario de memorizarlas, por ejemplo, quizás una docena de contraseñas o más. En otros casos, un usuario puede almacenar contraseñas en una única ubicación, tal como un cuaderno físico o un archivo electrónico que puede contener quizás todas las contraseñas del usuario.

- 20 Sin embargo, en el caso de que el usuario utilice una única contraseña para múltiples portales electrónicos, una única violación de la seguridad de un portal electrónico puede comprometer la información protegida por contraseña de la cuenta del usuario en cada uno de los múltiples portales electrónicos. En consecuencia, el usuario puede encontrarse en una situación desagradable de que se le facturen artículos que no ha pedido o de que se le facturen servicios que nunca recibirá. En otros casos, que puedan surgir quizás cuando un usuario registra las contraseñas en un archivo electrónico o en un cuaderno físico, la pérdida o la puesta en peligro bien del cuaderno o bien del archivo electrónico puede exponer al usuario a una responsabilidad económica significativa.

- 25 El documento US 2012/197806 A1 divulga sistemas, aparatos y procedimientos de uso de un mecanismo de comunicaciones acústicas para transmitir datos en forma de datos acústicos de un dispositivo móvil a un dispositivo electrónico. En una realización, un procedimiento para completar una adquisición con un vendedor usando un dispositivo móvil comienza con el envío desde el dispositivo móvil de un mensaje de solicitud a un servidor central a través de una interfaz de red. El dispositivo móvil recibe, entonces, una ficha desde el servidor central a través de la interfaz de red que confirma que se ha recibido un pago de la cantidad de la adquisición en la cuenta del vendedor. Esta ficha es traducida, entonces, en datos acústicos y transmitida del dispositivo móvil a un dispositivo electrónico que está asociado con la identificación de un vendedor.

- 35 El documento US 2011/258121 A1 proporciona un planteamiento para llevar a cabo transacciones por medio de un sistema de pago de base de fichas de audio. Un gestor de pago por audio recibe una solicitud, en un dispositivo, para el pago a un vendedor, incluyendo la solicitud una contraseña. En respuesta, el gestor de pago por audio recupera un número personal de identificación de un usuario del dispositivo, un identificador asociado con el usuario, un código de sesión, o una combinación de los mismos. El gestor de pago por audio genera, entonces, una ficha de audio en el dispositivo basada, al menos en parte, en la contraseña, el número personal de identificación, el identificador asociado con el usuario, el código de sesión, o la combinación de los mismos, y provoca, al menos en parte, la transmisión de la ficha de audio al vendedor para iniciar el pago.

Sumario de la invención

La invención está definida en las reivindicaciones independientes adjuntas.

- 45 En una implementación, un procedimiento para llevar a cabo una transacción puede incluir generar una ficha de un solo uso mediante un servidor de autorización, codificar la ficha de un solo uso que usa un código de control de errores, transportar la ficha de un solo uso del servidor de autorización a un dispositivo cliente, modular una señal de portadora para portar una carga útil de datos que contiene la ficha de un solo uso que usa una o más tecnologías y protocolos de comunicaciones de campo próximo, y comparar la ficha de un solo uso generada por el servidor de autorización con una ficha de un solo uso recibida por el dispositivo receptor. El procedimiento puede incluir, además, si se ha llevado a cabo una comparación con éxito, permitir que la transacción prosiga. El procedimiento puede incluir, además, si no se ha llevado a cabo una comparación con éxito, finalizar la transacción. Una ficha de un solo uso puede ser un número generado de forma aleatoria, resultado de operaciones criptográficas unidireccionales o de una variedad de otras operaciones matemáticas.

En otra implementación, un procedimiento para llevar a cabo una transacción segura puede incluir un dispositivo cliente que tiene uno o más procesadores para recibir una ficha de un solo uso y para transmitir una señal por medio

de un transmisor de comunicaciones de campo próximo acoplado con uno o más procesadores, en el que la señal representa una ficha de un solo uso.

5 En otra implementación, un módulo lógico para su uso con un navegador puede comprender un elemento de control para activar un receptor de comunicaciones de campo próximo para transmitir y/o recibir una señal acústica, un campo magnético variable en el tiempo, una señal de comunicación óptica, un código QR, o cualquier combinación de los mismos. El receptor de comunicaciones de campo próximo recibe una ficha de un solo uso para llevar a cabo una transacción.

Breve descripción de los dibujos

10 Se describen aspectos no limitantes y no exhaustivos con referencia a las siguientes figuras, en las que número similares de referencia hacen referencia a partes similares en todas las diversas figuras a no ser que se especifique algo distinto.

La Figura 1 es un diagrama de bloques que muestra un cliente y una plataforma informática para llevar a cabo una transacción segura según una realización.

15 La Figura 2 es un diagrama de flujo para un procedimiento para llevar a cabo una transacción segura por medio de una ficha de un solo uso según una realización.

Descripción detallada

20 En implementaciones, se puede crear un mecanismo que puede permitir que un usuario emplee un dispositivo personal de comunicaciones, tal como un teléfono celular, teléfono inteligente, u otro dispositivo que generalmente puede estar asociado con un individuo particular, así como otros dispositivos conectados a Internet para poder acceder rápida y fácilmente (por ejemplo, iniciar sesión) a portales electrónicos, terminales, puntos de venta, u otras entidades conectadas a Internet de forma sumamente segura. Después de iniciar sesión en un portal de comercio electrónico, por ejemplo, un usuario puede recibir una "ficha" de un solo uso en su dispositivo personal de comunicaciones generada por un servidor de autorización. Además, un servidor de autorización puede transportar una ficha coincidente o quizás complementaria, por ejemplo, al portal de comercio electrónico o quizás a un módulo lógico que puede ejecutarse, por ejemplo, en el portal de comercio electrónico. En otras implementaciones, la ficha puede ser retenida en el servidor de autorización en contraposición a ser transportada al portal de comercio electrónico.

30 Para iniciar una transacción, el dispositivo personal de comunicaciones puede emitir una señal, tal como una señal de audio, señal de comunicaciones de campo próximo, señal compatible con Bluetooth, u otro identificador que puede ser transportado por un terminal de punto de venta, ordenador portátil, de sobremesa, u otro que acceda al portal de comercio electrónico. Si el receptor recibe la señal, la información contenida en la señal puede ser transportada al servidor de autorización. El servidor de autorización puede, entonces, autorizar al usuario, que puede permitir que el usuario acceda al comercio electrónico por medio del portal de comercio electrónico. En implementaciones, si se ha producido la autenticación por parte del servidor de autorización, la ficha transportada al dispositivo personal de comunicaciones y la ficha coincidente o complementaria transportada al portal electrónico pueden ser eliminadas. De este modo, puede generarse una ficha "de un solo uso" con el fin de llevar a cabo la transacción y no se prevé que sea reutilizada en un momento posterior.

40 En la implementación, se puede garantizar la presencia únicamente de usuarios humanos reales que logran acceder a portales electrónicos seguros, y se puede impedir la posibilidad de que un usuario no humano, tal como un "ordenador zombi" u otra aplicación de soporte lógico que puede hacerse pasar por un usuario pueda acceder a un portal electrónico seguro. El uso de un dispositivo personal de comunicaciones, que puede requerir de forma inherente la manipulación inteligente por parte del usuario mientras interactúa simultáneamente con un portal electrónico, puede representar una característica que no puede ser fácilmente imitada por un ordenador zombi u otra aplicación de soporte lógico que se haga pasar por un usuario. En consecuencia, los sistemas de reto/respuesta, tales como "Captcha", en los que una respuesta generada por un ser humano a un reto generado por el portal electrónico puede usarse para garantizar la presencia de un usuario humano que interactúa con un portal electrónico, pueden sustituirse por realizaciones de la invención reivindicada.

50 Según se usa el término en la presente memoria, una "transacción" puede incluir meramente un intercambio de información segura, tal como la contraseña de los usuarios de "LinkedIn™", en el que el usuario que proporciona tal contraseña puede permitir que un usuario tenga ciertos privilegios como usuario registrado, se puede garantizar la seguridad de la información que pasa entre el usuario y el portal electrónico. Una "transacción" también puede incluir un intercambio comercial en el que bienes o servicios pueden obtenerse en respuesta a una promesa de pago por los bienes o servicios. En estos casos, así como en otros, una transacción puede llevarse a cabo sin requerir el uso de contraseñas u otros medios de autenticación por parte de una o más personas implicadas en la transacción. En lugar de contraseñas u otra información de autenticación, el intercambio de la ficha de un solo uso descrita en la presente memoria puede ser lo único que se requiere para autenticar a un usuario implicado en una transacción.

Además, en implementaciones, puede no requerirse que un usuario recuerde contraseñas, lo cual puede permitir que un usuario disfrute adicionalmente de una experiencia de compra en línea. En ciertas implementaciones, un portal de comercio electrónico, por ejemplo, puede no requerir almacenar una contraseña, credenciales u otra información personal de un usuario, lo cual puede permitir que el portal de comercio electrónico se centre en proporcionar bienes y servicios a un precio competitivo. En consecuencia, dado que puede ya no requerirse que los portales de comercio electrónico, por ejemplo, almacenen información personal correspondiente potencialmente con miles o millones de clientes, se puede impedir que se produzca el robo de la información privada de los usuarios.

Además, en implementaciones, un usuario puede no requerir establecer una cuenta con una entidad en línea, tal como un portal electrónico seguro o un portal de comercio electrónico, dado que establecer una cuenta es principalmente una herramienta para la autenticación posterior del usuario. Se puede lograr la autenticación del usuario, al menos en parte, por medio de la metodología segura de ficha de un solo uso descrita en la presente memoria. En implementaciones, un usuario puede iniciar sesión por medio de la metodología segura de ficha de un solo uso descrita en la presente memoria y puede ser autenticado sin requerir que la entidad en línea almacene, mantenga y garantice la seguridad de la información de autenticación y potencialmente sensible de los usuarios. Sin embargo, en algunas implementaciones, un usuario puede permitir que la entidad en línea, tal como un portal electrónico de transacciones, solicite el nombre u otra información personal para permitir que se cree un registro de gestión de relación con el cliente, lo cual puede ser deseable o necesario para completar una transacción y, de ese modo, que sea reconocido en una visita subsiguiente al portal electrónico. Alternativamente, un usuario puede mantener el anonimato, aunque siga estando autenticado como un usuario legítimo. La información personal puede ser mantenida por el servidor de autorización y puede ser pasada al portal electrónico de transacción sin la necesidad de que el usuario introduzca o vuelva a introducir información de identificación, tal como contraseñas, cuando usa diversos portales electrónicos. En estas realizaciones, la información personal puede ser recogida por el servidor de autorización como parte de una instalación inicial de la aplicación del usuario y verificación inicial del usuario. La verificación inicial del usuario puede ser un proceso realizado una sola vez, el cual requiere que un usuario presente la información de identificación personal, que puede incluir sin limitación: nombre, dirección, número de la Seguridad Social, información de la tarjeta de crédito para transacciones, otra información bancaria, información secreta compartida (por ejemplo, apellido de soltera de la madre, segundo nombre del padre, etc.) para su autenticación posterior, espectrograma de la voz, huella de la palma de la mano, reconocimiento de iris u otras características biométricas únicas al usuario, que puede ser requerida para una autenticación del usuario de alto nivel por parte de las entidades en línea u otras entidades que requieren la autenticación del usuario. Una vez que el usuario ha proporcionado la información y, por lo tanto, está autenticado, se puede transmitir una aplicación de dispositivo móvil al usuario. La aplicación puede comprender un número de serie único que identifica de forma unívoca al usuario y puede ser enviada al servidor de autorización cada vez que se inicie una sesión o una transacción por parte del usuario, pudiéndose usar el número de serie único para identificar al usuario y, junto con la ficha de un solo uso, pueden ser usados para autorizar inicios de sesión a portales electrónicos o transacciones en portales de comercio electrónico, por ejemplo. El número de serie único puede combinarse con la identificación del dispositivo personal de comunicaciones de muchas formas tal como una o más operaciones matemáticas que incluyen, sin limitación, funciones de clave calculada criptográfica unidireccional, tales como MD5, SHA-2, por nombrar algunos ejemplos.

Según se ha mencionado anteriormente, en implementaciones, pueden usarse comunicaciones de campo próximo para comunicar una ficha, por ejemplo, de un dispositivo personal de comunicaciones a un portal participante de comercio electrónico, por ejemplo. En consecuencia, las comunicaciones de campo próximo pueden operar usando una amplia variedad de tecnologías de comunicaciones de corto alcance. Por ejemplo, la tecnología de comunicaciones de campo próximo puede comprender el uso de una señal de audio, que puede comprender una señal que puede comenzar a una frecuencia y terminar en otra frecuencia (es decir, un “chirrido”) o una variedad de técnicas de FM, AM, espectro de propagación u otras usadas en sistemas de telecomunicaciones hoy en día. Las comunicaciones de campo próximo pueden comprender el uso de un acoplamiento inductivo, en el cual puede operar un campo magnético variable en el tiempo generado en una primera ubicación, tal como un dispositivo cliente, y puede ser percibido o detectado en una segunda ubicación, tal como un ordenador portátil, de sobremesa, un terminal de punto de venta, un dispositivo informático portátil, etcétera, tras lo cual puede operarse una aplicación de comercio electrónico (que puede incluir un navegador). En implementaciones, la segunda ubicación y la primera ubicación pueden estar separadas entre 1,0 y 20,0 cm, por ejemplo. Sin embargo, se debería hacer notar que, en otras implementaciones, los campos magnéticos variables en el tiempo pueden ser detectados en ubicaciones a más de 20,0 cm, por ejemplo, y a menos de 1,0 cm, por ejemplo.

Las comunicaciones de campo próximo también pueden comprender el uso de dígitos binarios representados por frecuencias particulares de un espectro de audio. En un ejemplo posible entre numerosas implementaciones posibles, un estado lógico que se corresponde con un “0” binario puede ser transportado usando un tono de 400 Hz, por ejemplo. Un estado lógico que se corresponde con un “1” binario puede ser transportado usando un tono de 1000 Hz, por nombrar dos ejemplos. Además, el código de control de errores tal como códigos Hamming, códigos Bose Chaudhuri-Hocquenghem, códigos Reed Solomon, redundancia cíclica, o cualquier tecnología de código de control de errores, que puede ser aplicada por un servidor de autorización y/o un dispositivo cliente a los dígitos binarios que comprenden la ficha de un solo uso. En consecuencia, puede garantizarse la integridad de una ficha

intacta de un solo uso, quizás incluso cuando sea transmitida usando una modulación de portadora electromagnética, sónica o de inducción magnética y transmitida por canales ruidosos.

La Figura 1 es un diagrama de bloques que muestra un cliente y una plataforma informática para llevar a cabo una transacción segura según una realización. En la Figura 1, el dispositivo 15, puede, por ejemplo, representar un dispositivo personal de comunicaciones, tal como un teléfono celular, teléfono inteligente, u otro dispositivo generalmente llevado o portado en la persona de un usuario. En una implementación, el dispositivo 15 puede tener conectividad tanto a la nube 80 como, por ejemplo, a través de la interfaz 35 de Internet. El usuario 10 puede operar el dispositivo 15 por medio de la aplicación 20 de interfaz del usuario para llevar a las diversas operaciones facilitadas por el dispositivo 15, tal como enviar y recibir comunicaciones de teléfono móvil, enviar mensajes de texto, navegación personal, juegos, redes sociales, etcétera.

En una implementación, la aplicación 20 de usuario puede representar una aplicación segura que recibe una ficha de transacción de un solo uso, por ejemplo, del servidor 110 de autorización por medio de la nube 80 y una interfaz 35 de Internet. En implementaciones particulares, el servidor 110 de autorización puede comunicarse con el servidor 100 del banco y/o un servidor 120 de la tarjeta de crédito u otro proceso de pago usando, por ejemplo, protocolos estandarizados tal como OpenID, OAuth, SAML, por nombrar unos posibles protocolos de comunicaciones. En una implementación, cuando se ha de iniciar una transacción entre el dispositivo 15 y el dispositivo 50, el servidor 110 de autorización transporta una ficha complementaria y/o coincidente de un solo uso al dispositivo 50. En una implementación, las fichas de un solo uso transportadas al dispositivo 15 y al dispositivo 50 pueden no ser idénticas, pero pueden ser, en su lugar, complementarias, de forma que cuando se combinan las fichas de un solo uso del dispositivo 15 y el dispositivo 50, resulta una solución determinista. En un ejemplo posible entre muchos, se pueden sumar entre sí las fichas de un solo uso del dispositivo 15 y del dispositivo 50 para producir un "síndrome", que puede ser igual a un "0" binario o se pueden sumar entre sí para producir un resultado diferente. Se debe hacer notar, sin embargo, que aunque se puedan sumar las fichas de un solo uso, al menos en una implementación, en otras implementaciones se pueden restar entre sí las fichas de un solo uso, multiplicarse una por otra, convolucionarse, o ser sometidas a cualquier otra operación lógica o matemática y el contenido reivindicado no está limitado en este sentido.

Para identificar al usuario 10 del dispositivo 15, un transmisor 25 de comunicaciones de campo próximo del dispositivo puede emitir una señal que puede ser detectada por un sensor 60 de comunicaciones de campo próximo del dispositivo 50. Tras recibir una señal, un decodificador 65 puede decodificar la señal recibida. En consecuencia, un decodificador 65 puede llevar a cabo una desmodulación de una señal en un dominio de audio, una conversión de señales inductivas y/o magnéticas a una señal digital, u otra conversión que permita que los estados de información transportados sean transportados por el transmisor 25 de comunicaciones de campo próximo mediante la interfaz 78 de Internet al servidor 110 de autorización.

En consecuencia, en implementaciones, si el usuario 10 se encuentra, por ejemplo, comprando en un portal de comercio electrónico, una cesta de compra u otro recipiente virtual puede ser mostrado al usuario 10 por medio de la aplicación 70 del usuario, que puede incluir un navegador, que se ejecuta en el dispositivo 50. Si el usuario 10 ha seleccionado un artículo para su adquisición, por ejemplo, el transmisor 25 de campo próximo del dispositivo 15 puede codificar una ficha de transacción de un solo uso como una carga útil de datos, y modular la carga útil por medio de una técnica de modulación para ser recibida por el sensor 60 de comunicación de campo próximo del dispositivo 50. El sensor 60 de comunicación de campo próximo puede desmodular la señal recibida para que sea decodificada por el decodificador 65 y transmitida mediante la interfaz 78 de Internet a la nube 80 y al servidor 110 de autorización. Si el servidor 110 de autorización autentifica la ficha de un solo uso, el servidor de autorización puede indicar a la aplicación 70 del usuario que se ha autorizado la transacción. La autorización puede indicar una garantía al operario del portal de comercio electrónico, por ejemplo, de que se ha completado la transacción y el artículo adquirido puede ser enviado al usuario 10, por ejemplo.

Aunque la transacción identifica específicamente un comercio electrónico, nada evita otros tipos de transacciones, tales como bancarias, pago de facturas, o cualquier otro tipo de transacción en el que la seguridad puede ser potenciada por medio de una generación de una ficha de un solo uso en un primer dispositivo, tal como el dispositivo 15, que puede ser recibida por un segundo dispositivo, tal como el dispositivo 50. En consecuencia, el contenido reivindicado no está limitado en este sentido. Además, una transacción puede operar en una dirección opuesta a la dirección descrita anteriormente. Por ejemplo, los dispositivos 15 y 50 pueden representar, por ejemplo, teléfonos inteligentes u otros dispositivos capaces de realizar una transacción electrónica. En una implementación, el usuario 10 puede querer transmitir un pago al usuario 75. En tal implementación, el servidor 110 de autorización puede generar una ficha de un solo uso para su uso por parte de la aplicación 20 de interfaz del usuario. En tal caso, el usuario 10 puede seleccionar una cantidad en euros, por ejemplo, que ha de ser pagada a un usuario 75. El servidor 110 de autorización puede generar una ficha de un solo uso para ser transmitida por el dispositivo 15 para su transmisión mediante el transmisor 25 de comunicaciones de campo próximo. Si el sensor 60 de comunicación de campo próximo recibe la ficha modulada de un solo uso, la ficha de un solo uso puede ser comparada con una ficha de un solo uso transmitida por el servidor 110 de autorización al dispositivo 50. En el caso de que la comparación indique una coincidencia entre las fichas de un solo uso, se puede transmitir el pago de una cuenta bancaria asociada con el usuario 10 a una cuenta bancaria asociada con el usuario 75.

La Figura 2 es un diagrama de flujo de un procedimiento para llevar a cabo una transacción segura por medio de una ficha de un solo uso según una realización. En el bloque 210, un usuario, tal como el usuario 10 de la Figura 1, asociado con el dispositivo 1 (200) se aproxima al dispositivo 2 (400). El dispositivo 2 puede conectar un portal electrónico deseado, tal como un portal de comercio electrónico. En 220, el dispositivo 2 (400), que quizás pueda estar asociado con un portal de comercio electrónico, muestra una opción para iniciar sesión de forma segura por medio de comunicaciones de campo próximo. En 225, un usuario asociado con el dispositivo 1 (200) puede aceptar la opción y activar una aplicación de cliente de comunicaciones de campo próximo que puede ser ejecutada en el dispositivo 1 (200). El dispositivo 2 (400) puede comenzar a monitorizar comunicaciones de campo próximo para detectar una identificación de inicio de sesión del usuario 1, tal como en el bloque 230. El dispositivo 2 puede, al menos en algunas implementaciones, comprender una capacidad para activar un receptor de comunicaciones de campo próximo, tal como una entrada de micrófono, un sensor para detectar campos magnéticos variable en el tiempo, etcétera.

En el bloque 230, un usuario asociado con el dispositivo 1 (200) puede iniciar sesión en el portal de comercio electrónico, por ejemplo. El dispositivo 1 (200) puede solicitar una identificación de inicio de sesión, por ejemplo, de un servidor de autorización, tal como un servidor 300 de autorización. En respuesta, el servidor 300 de autorización, en el bloque 240, puede recibir una solicitud de un inicio de sesión del dispositivo 1 (200). En 245, un servidor (300) de autorización puede autenticar el dispositivo 1 (200) mediante la solicitud, por ejemplo en el bloque 245, de una autenticación biométrica almacenada en el servidor (300) de autorización, de un usuario asociado con el dispositivo 1 (200). Tal autenticación biométrica puede incluir, sin limitación, identificación biométrica de la retina, huella de la palma de la mano, espectrograma de la voz, articulación de una palabra clave, huella dactilar, u otra identificación. La mayoría de dispositivos modernos personales de comunicaciones incluyen todos una cámara y un micrófono en los que una identificación biométrica de la retina, una huella de la palma de la mano, un espectrograma de la voz, una articulación de una palabra clave, una huella dactilar, u otras características biométricas, pueden ser capturadas, analizadas, y enviadas al servidor de autorización para su verificación. En el bloque 250, el servidor 300 de autorización puede generar un código de transacción de un solo uso para su uso por parte del dispositivo 1 (200). En el bloque 255, el dispositivo 1 (200) puede recibir la ficha de un solo uso del servidor 300 de autorización.

En el bloque 260, el dispositivo 1 (200) puede transmitir una ficha de un solo uso que ha de ser recibida por el dispositivo 2 (400) por medio de un receptor de comunicaciones de campo próximo. En 265, el dispositivo 2 (400) puede recibir la ficha de un solo uso. En el bloque 270, el dispositivo 2 (400) puede transmitir el identificador de transacción de un solo uso junto con cualquier otra información de autenticación al servidor 300 de autorización. En el bloque 275, el servidor 300 de autorización puede comparar fichas recibidas de un solo uso generadas por el servidor de autorización con una ficha de un solo uso recibida por el dispositivo 2 (400) en el bloque 265. En el caso de que la comparación (275) dé lugar a una coincidencia positiva entre las fichas generada y recibida de un solo uso, puede llevarse a cabo el bloque 280 en el que una transacción puede ser autorizada por medio de un servidor (300) de autorización. En el bloque 285, el dispositivo 1 (200) puede recibir del servidor 300 de autorización la autorización para que se produzca la transacción.

En el caso de que la comparación del bloque 275 llevada a cabo por el servidor 300 de autorización no indique una coincidencia entre las fichas generada y recibida de un solo uso, puede finalizarse una transacción, tal como en el bloque 297. Tal finalización puede desactivar o borrar las fichas de un solo uso, de forma que cualquier transacción subsiguiente pueda requerir la generación de una ficha nueva de un solo uso. En el bloque 285, el dispositivo 1 (200) puede recibir un aviso de finalización. En el bloque 299, un portal electrónico que puede corresponderse con un portal de comercio electrónico, también puede recibir un aviso de finalización.

En otras implementaciones, un módulo/aplicación de soporte lógico del dispositivo personal de comunicaciones u otro dispositivo que contiene un módulo/aplicación de soporte lógico (móvil, ordenador portátil, de sobremesa o un terminal o servidor/ordenador) que incluye una capacidad de comunicaciones de campo próximo puede comunicarse con otro dispositivo (móvil, ordenador portátil, de sobremesa, cualquier terminal o servidor/ordenador) que comprende una capacidad de comunicaciones de campo próximo por medio de un enlace de comunicaciones de campo próximo. Los dispositivos también pueden comunicarse con un servidor de autorización por medio de Internet. En implementaciones, pueden estar implicados más de dos dispositivos en la transacción. Entonces, el servidor de autorización implementa, monitoriza y controla un protocolo seguro de inicio de sesión/transacción descrito anteriormente. De forma alternativa, una o más de las partes implicadas en el inicio de sesión o en la transacción seguros pueden ser representadas por un portal electrónico dedicado en una configuración sin clientes.

Las implementaciones pueden usar un dispositivo inteligente personal de comunicaciones con una aplicación móvil que ha de ser cargada en él que puede usar comunicaciones de campo próximo para comunicarse con un dispositivo/ portal electrónico que pueda recibir o transmitir señales de comunicaciones de campo próximo. Esto puede implementarse como dispositivos habilitados para las comunicaciones de campo próximo de radiofrecuencia o a través del uso de la transmisión/recepción sónica de datos que no requiere comunicaciones de campo próximo basadas en radiofrecuencia, sino que usa únicamente los micrófonos y altavoces existentes en los dispositivos personales de comunicaciones, ordenadores portátiles, de sobremesa y terminales.

En otras implementaciones, un procedimiento para transportar una ficha de transacción de un solo uso entre partes que interactúan emplea uno o más códigos de barra uni o bidimensionales que pueden ser mostrados por un dispositivo habilitado y ser fotografiados por un dispositivo personal de comunicaciones del usuario y ser analizados por una aplicación procesadora de señales digitales de lectura de códigos de barra. En otras implementaciones, uno o más códigos de barra uni o bidimensionales pueden ser mostrados en un dispositivo personal de comunicaciones del usuario y ser fotografiados por un dispositivo o dispositivos habilitados y ser analizados mediante aplicaciones procesadoras de señales digitales de lectura de códigos de barra.

La transmisión de la ficha de transacción de un solo uso puede ser de un usuario a un dispositivo habilitado o de un dispositivo habilitado al usuario, siempre y cuando todas las partes implicadas en una transacción obtengan la misma ficha de transacción de un solo uso y sean capaces de enviar una ficha de transacción de un solo uso de forma concurrente o dentro de un espacio de tiempo corto limitado, por ejemplo, al servidor de autorización para su autenticación. En un ejemplo, una ficha de transacción de un solo uso puede “sobrevivir” durante quizás, una fracción de un segundo. En consecuencia, un servidor de autorización puede generar una ficha de transacción de un solo uso y una ficha coincidente o complementaria para su uso por parte del portal electrónico. En una implementación, tanto la ficha de transacción de un solo uso como la ficha coincidente o complementaria para su uso por parte del portal electrónico, en la que deben usarse ambas, por ejemplo, en medio segundo o menos, aunque el contenido reivindicado no está limitado en este sentido. En algunas implementaciones, una ficha de transacción de un solo uso y una ficha coincidente o complementaria pueden sobrevivir durante una fracción de segundo, unos segundos, o quizás hasta unos minutos o un periodo más largo de tiempo. La vida corta de una ficha y su uso único garantiza una seguridad contra una variedad de ataques de “intermediarios” en los que se intercepta, decodifica o registra la comunicación por parte de un atacante para su uso subsiguiente en una transacción ilegal. El uso único y la vida corta garantiza que la ficha solo pueda usarse una vez en la transacción original y que, a continuación, ya no sea válida.

De forma similar, la transmisión del número de transacción puede ser de usuario a usuario, dispositivo personal de comunicaciones a dispositivo personal de comunicaciones, para proporcionar la autenticación mutua de los usuarios y para permitir que se intercambie la información entre usuarios o que se ejecute una transacción entre usuarios.

Se debería hacer notar que ya existen muchas topologías para pasar fichas de un solo uso a dispositivos y fichas complementarias o coincidentes a los portales electrónicos receptores u otras entidades de procesamiento. En otro ejemplo, una ficha puede ser generada en un servidor de autorización y ser transportada a un dispositivo personal de comunicaciones del usuario. Si la ficha de un solo uso ha sido recibida por un dispositivo personal de comunicaciones, la ficha puede ser transportada por medio de comunicaciones de campo próximo a un navegador, que puede mostrar un portal electrónico por medio del uso de módulos adicionales de navegador tal como Flash, u otro módulo adicional habitual u otros reproductores multimedia para visualizar animaciones y/o películas usando programas informáticos tales como un navegador de páginas electrónicas. En una implementación, en lugar de Flash, un navegador puede ejecutar HTML-5. En cualquier caso, por ejemplo, un micrófono puede ser habilitado por el módulo adicional de navegador, tal como Flash, HTML-5, o un reproductor multimedia, en el que el micrófono puede acoplarse con un procesador de señales digitales, que puede recuperar la ficha recibida de un solo uso, quizás transportada por medio de una señal acústica. El procesador de señales digitales puede recuperar o extraer la ficha de un solo uso de la señal, y transportar la ficha recibida a un servidor de autorización, de forma que la ficha recibida pueda ser comparada con la ficha generada originalmente por el servidor, autenticando, así, ambos lados de la transacción y autorizando la transacción, por ejemplo.

En ciertas implementaciones, puede mostrarse en una ventana del navegador un elemento de control, tal como un gráfico, un icono, u otra forma de enlace activo. Un usuario que busca la autenticación puede identificarse, entonces, en un servidor de autorización por medio de la activación del enlace, lo que puede permitir la transmisión de parámetros de voz extraídos, y/o una ficha de un solo uso, al servidor de autorización. En implementaciones particulares, sin embargo, una aplicación adecuada de navegación tal como HTML5, Flash, u otra aplicación puede establecer un enlace a un servidor de autorización sin la necesidad de mostrar un gráfico, un icono, u otra forma de enlace activo en una ventana del navegador. En tal caso, un dispositivo móvil del usuario, que puede comprender un teléfono celular, teléfono inteligente, u otro dispositivo portátil de comunicaciones, puede operar una aplicación de autenticación para recibir una ficha de un solo uso, por ejemplo, que puede ser generada por una aplicación adecuada de navegador. En implementaciones particulares, una ficha de un solo uso puede ser transmitida a través de los altavoces de un dispositivo informático portátil, por ejemplo, para su recepción por el dispositivo móvil del usuario.

Una ficha de un solo uso, que puede ser generada por un navegador, puede comprender una o más de una señal acústica, una señal de comunicaciones de campo próximo de tipo electromagnético, una señal óptica de comunicaciones, un código QR, u otra técnica de señalización, o cualquier combinación de los mismos, que puede ser generada por una aplicación de navegación, y recibida por un dispositivo móvil. Una aplicación de navegación puede recibir, por ejemplo, una ficha codificada de un solo uso para su transmisión a un servidor de autorización para su conversión a una señal de campo próximo que puede ser recibida por un dispositivo móvil del usuario. Además de los parámetros extraídos de una señal de campo próximo generada por un navegador, por ejemplo, un

dispositivo móvil del usuario puede transportar adicionalmente parámetros del dispositivo móvil, tales como el número de ID de la aplicación de autenticación, el número de ID del dispositivo, el perfil del dispositivo, etcétera, que pueden ser utilizados, por ejemplo, por un servidor de autorización para identificar el dispositivo móvil que participa en un proceso de autenticación. En consecuencia, una interfaz del usuario de una ventana del navegador, por ejemplo, puede ser simplificada porque un usuario puede evitar interactuar con un gráfico, un icono, u otro enlace activo para permitir la transmisión de una ficha de un solo uso a un servidor del navegador, que puede funcionar como un servidor de autorización.

En otra topología, una ficha puede ser generada por un proceso en segundo plano que puede ejecutarse como parte de un programa de navegación (que se ejecuta, por ejemplo, en un "servidor" del portal electrónico), que se ejecuta como código o secuencia de instrucciones en un módulo adicional de navegador, tal como Flash, HTML-5, o un reproductor multimedia que está ejecutado en un segundo plano o en un primer plano. La ficha generada por el servidor del portal electrónico puede ser enviada a un servidor de autorización. La ficha de un solo uso puede ser transportada por el servidor de autorización a un dispositivo personal de comunicaciones, pudiendo el dispositivo personal de comunicaciones, quizás por medio de comunicaciones de campo próximo, transmitir la ficha de un solo uso a un navegador que ejecuta el proceso en segundo plano. En esta implementación, el proceso de autenticación (es decir, la comparación de la ficha de un solo uso recibida del dispositivo personal de comunicaciones con la ficha de un solo uso generada por el proceso en segundo plano del navegador) puede llevarse a cabo usando el navegador, quizás por medio del propio proceso de autenticación del navegador. En otros casos, la autenticación puede llevarse a cabo en un servidor de autorización.

En otra topología, un navegador de portales electrónicos puede hacer uso de comunicaciones de campo próximo para transmitir una ficha de un solo uso a un dispositivo personal de comunicaciones. El dispositivo personal de comunicaciones y ese navegador de portales electrónicos pueden simultánea, o casi simultáneamente, transportar ambos la ficha de un solo uso a un servidor de autorización para su comparación.

En otra topología, un navegador de portales electrónicos puede abrirse y/o ejecutarse en un dispositivo personal de comunicaciones, y un usuario del dispositivo personal de comunicaciones puede iniciar sesión en un comercio electrónico u otro portal electrónico que requiere autenticación para que se lleve a cabo una transacción. En este escenario, el comercio electrónico u otro portal electrónico que requiere autenticación puede abrirse en una ventana del navegador, por ejemplo, en el dispositivo personal de comunicaciones y puede ser capaz de comunicarse por medio del navegador o del módulo adicional del navegador (Flash, HTML, HTML 5, etc.), con la aplicación del dispositivo personal de comunicaciones diseñada o adaptada para gestionar la metodología de ficha de un solo uso descrita anteriormente. Un usuario puede pulsar un botón del portal electrónico (por ejemplo, un botón de radio) que solicita autenticación. En respuesta, el navegador puede enviar una solicitud a la aplicación del dispositivo personal de comunicaciones. La aplicación del dispositivo personal de comunicaciones puede recibir la solicitud y, en respuesta, puede solicitar que se envíe una ficha de un solo uso por medio del servidor de autorización al comercio electrónico u otro portal electrónico que requiere autenticación, abierta y/o ejecutada actualmente en el navegador. El comercio electrónico u otro portal electrónico que requiere autenticación, abierto actualmente en el navegador puede recibir la ficha solicitada del servidor de autorización y, entonces, envía la ficha de un solo uso a la aplicación del dispositivo personal de comunicaciones. En respuesta, el dispositivo personal de comunicaciones puede recibir la ficha de un solo uso, enviar la ficha de un solo uso de nuevo al servidor de autorización en el que se puede comparar la ficha con la ficha transportada recientemente al comercio electrónico u a otro portal electrónico que requiere autenticación, abierto y/o ejecutado actualmente en el navegador. Si hay una coincidencia u otra comparación, el usuario puede ser autorizado además ante el portal de comercio electrónico.

Otros canales de comunicaciones entre el navegador y la aplicación del dispositivo personal de comunicaciones, que puede estar diseñada o adaptada para gestionar la metodología de ficha de un solo uso, pueden ser aprovechados para completar el bucle de entrega de la ficha y de coincidencia de fichas necesario para la autenticación del usuario y del portal electrónico. El navegador puede enviar información al altavoz del dispositivo personal de comunicaciones que puede monitorizarse directamente o por medio del micrófono del dispositivo personal de comunicaciones por medio de la aplicación del dispositivo personal de comunicaciones diseñada para gestionar la metodología de ficha de un solo uso, o adaptada a la misma. En este caso, la información que contiene la ficha puede codificarse usando una modulación de señal acústica. En otra implementación, la aplicación del dispositivo personal de comunicaciones puede estar diseñada para gestionar la metodología de ficha de un solo uso, o adaptada a la misma, puede enviar información al altavoz del dispositivo personal de comunicaciones que puede monitorizarse directamente o por medio del micrófono del dispositivo personal de comunicaciones por parte del navegador. La ficha de un solo uso puede ser pasada por medio del navegador a la aplicación o por medio de la aplicación al navegador, para acabar en el servidor de autorización para su comparación. Alternativamente, la comparación de fichas puede ser realizada por el navegador, el servidor del portal de comercio electrónico o la aplicación del dispositivo personal de comunicaciones diseñada para gestionar la metodología de ficha de un solo uso.

Alternativamente, el navegador y la aplicación pueden comunicarse mediante escritura y lectura en las cookies del navegador y de las mismas, que pueden ser accesibles a la aplicación del dispositivo personal de comunicaciones diseñada para gestionar la metodología de ficha de un solo uso.

Según se ha mencionado anteriormente, las implementaciones pueden ser útiles para sustituir parcial, o incluso completamente, las técnicas convencionales de verificación del usuario tales como "Captcha", que deniegan el acceso al portal electrónico a los rastreadores zombi de páginas electrónicas garantizando que la entidad que accede al portal electrónico es un ser humano. Los esquemas "Captcha" pueden comprender, por ejemplo, una o más palabras o frases mostradas o audibles presentadas a un usuario. En respuesta, un usuario puede introducir la frase Captcha recibida o mostrada en un navegador del portal electrónico. El portal electrónico puede comparar, entonces, la frase Captcha generada con la frase Captcha recibida y puede realizarse la autenticación. Sin embargo, muchos usuarios encuentran que este proceso es difícil y es propenso a errores, dado que las palabras o frases mostradas o audibles pueden ser indescifrables visualmente o de forma audible y, por lo tanto, pueden ser difíciles de interpretar y/o recitar. En muchos casos, los usuarios deben pasar varias iteraciones hasta que se pueda completar con éxito la autenticación.

La autenticación biométrica también puede ser usada para autenticar transacciones de mayor valor, o quizás cuando se pierde el dispositivo personal de comunicaciones del usuario o lo roban. En tal implementación, un portal electrónico o servidor de autorización puede requerir que un usuario se autentique por medio de un identificador biométrico, tal como un espectrograma de la voz, magnético, barrido de la palma de la mano, o quizás contestar una pregunta secreta, tal como "¿Cuál fue la marca y modelo de tu primer coche?"

Aunque se han definido las anteriores implementaciones y realizaciones, estas son meramente ilustraciones de los conceptos reivindicados.

REIVINDICACIONES

1. Un procedimiento para llevar a cabo una transacción segura, que comprende:

generar, mediante un servidor (110, 300) de autorización, una ficha de un solo uso codificada usando un código de control de errores;

transportar la ficha codificada de un solo uso desde el servidor (110, 300) de autorización hasta un dispositivo cliente (15, 200), incluyendo dicho dispositivo cliente (15, 200) un navegador que puede ejecutar una aplicación usando comunicaciones de campo próximo y un enlace en el que se puede pinchar para conectar la aplicación de navegación al servidor (110, 300) de autorización;

transportar, mediante altavoces del dispositivo cliente (15, 200), por medio de una señal de audio, la ficha codificada de un solo uso para un dispositivo receptor (50, 400) que incluye un dispositivo móvil;

recibir la ficha codificada de un solo uso por medio de un micrófono del dispositivo receptor (50, 400);

comparar, mediante el servidor (110, 300) de autorización, la ficha de un solo uso generada por el servidor (110, 300) de autorización con la ficha codificada de un solo uso recibida por el dispositivo receptor (50, 400) realizando una operación matemática; y

permitir, mediante el servidor (110, 300) de autorización, que la transacción segura prosiga o finalizar la transacción segura en función de dicha comparación.

2. El procedimiento de la reivindicación 1, que comprende, además, comparar la información biométrica de un usuario con la información biométrica almacenada en el servidor de autorización.

3. El procedimiento de la reivindicación 1, en el que la señal de audio comprende un chirrido acústico o una señal acústica que usa una o más frecuencias de audio.

4. El procedimiento de la reivindicación 1, en el que uno o más del servidor de autorización y del dispositivo cliente aplican el código de control de errores a la ficha de un solo uso.

5. El procedimiento de la reivindicación 1, en el que el enlace de la aplicación de navegación es activado automáticamente si se abre una nueva página electrónica.

6. El procedimiento de la reivindicación 1, en el que la operación matemática consiste en una suma, una resta, una convolución, una comparación y/o una correlación.

7. Un sistema para llevar a cabo una transacción segura, que comprende:

un servidor (110, 300) de autorización que comprende un generador de fichas para generar una ficha de un solo uso codificada usando el código de control de errores y una interfaz capaz de transportar la ficha generada codificada de un solo uso; y

un dispositivo receptor (50, 400) que incluye un dispositivo móvil;

y comprendiendo el sistema, además:

un dispositivo cliente (15, 200) que incluye:

- un navegador que puede ejecutar una aplicación usando comunicaciones de campo próximo,

- un enlace en el que se puede pinchar para conectar la aplicación de navegación a dicho servidor (110, 300), y

- altavoces para transportar una señal de audio que comprende la ficha codificada de un solo uso a dicho dispositivo receptor (50, 400),

en el que el servidor (110, 300) de autorización está configurado, además, para comparar la ficha de un solo uso generada por el servidor (110, 300) de autorización con la ficha codificada de un solo uso recibida por medio de un micrófono del dispositivo receptor (50, 400) realizando una operación matemática, y para permitir que la transacción segura prosiga o finalizar la transacción segura en función de dicha comparación.

8. El sistema de la reivindicación 7, en el que la señal de audio comprende un chirrido acústico o una señal acústica que usa una o más frecuencias de audio.

FIG. 1

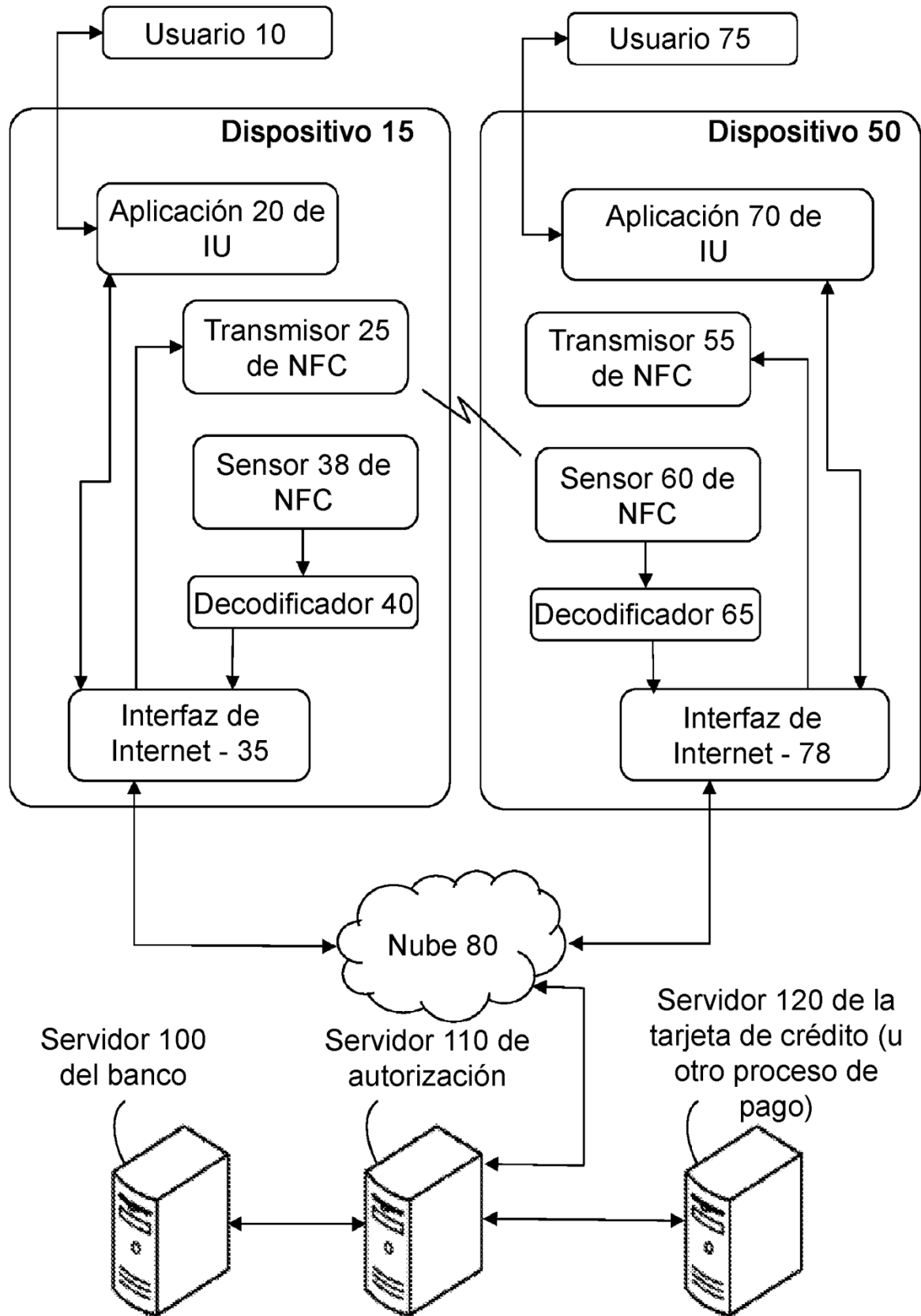


FIG. 2

