(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 596 754**

(21) Número de solicitud: 201531014

(51) Int. CI.:

G06Q 20/00 (2012.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

10.07.2015

(43) Fecha de publicación de la solicitud:

11.01.2017

(71) Solicitantes:

CONSORCIO DE TRANSPORTES DE BIZKAIA (100.0%)
Ugasko 5 bis - 1º
48014 Bilbao (Bizkaia) ES

(72) Inventor/es:

FERNÁNDEZ CASANELLAS, Daniel;
ISASI GOMENDIOURRUTIA, Juan Luis y
ELUSTONDO GONZÁLEZ-PINTO , Javier

(74) Agente/Representante:

TRIGO PECES, José Ramón

(54) Título: **Método y sistema de recarga de tarjetas inteligentes para su uso como billetes de transporte, a través de un terminal con NFC**

(57) Resumen:

Sistema (1) y método para la recarga de tarjetas inteligentes (10) para su uso como billetes de transporte. El sistema (1) comprende un servidor (20), al menos un terminal de usuario (30) con tecnología NFC, por ejemplo un teléfono móvil, y al menos una tarjeta inteligente (10). Para efectuar la recarga, el terminal de usuario (30) establece comunicaciones NFC con la tarjeta inteligente (10) de un usuario (99) y comunicaciones remotas con el servidor (20), actuando de intermediario para establecer una autenticación mutua entre ambos. El sistema (1) permite al usuario (99) adquirir un título de transporte desde su teléfono móvil y utilizar dicho teléfono móvil como terminal de recarga de la tarjeta inteligente (10) de forma cómoda y segura. Adicionalmente, se elimina la necesidad de disponer de terminales de recarga convencionales reduciéndose el coste del mantenimiento del sistema.

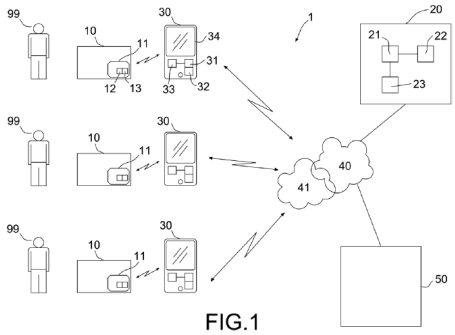

FIG.1

ES 2 596 754 A1

MÉTODO Y SISTEMA DE RECARGA DE TARJETAS INTELIGENTES PARA SU USO COMO BILLETES DE TRANSPORTE, A TRAVÉS DE UN TERMINAL CON NFC

DESCRIPCIÓN

Sector de la técnica

La invención se refiere a un método y a un sistema de recarga de billetes de transporte en tarjetas inteligentes, en el cual la recarga se realiza a través de un teléfono móvil u otro terminal de usuario portátil inalámbrico dotado de tecnología “Near Field Communication” (NFC).

Estado de la técnica

En los sistemas de transporte público se conocen múltiples formas de presentación de los billetes de transporte, así como de formas de pago.

Tradicionalmente, se han ofrecido a los viajeros billetes en formato físico o de papel, de ida o de ida y vuelta entre un origen y un destino, a cambio de un pago generalmente en metálico o con tarjeta de crédito. También ha sido habitual la venta de bonos multiviaje o abonos con carácter temporal, válidos entre unas fechas determinadas entre un origen y un destino igualmente en formato físico o de papel, a cambio también de un pago generalmente en metálico o con tarjeta de crédito.

Con el desarrollo de las tecnologías de la información, han aparecido gradualmente billetes soportados en formato electrónico. Por ejemplo, se conoce el uso de tarjetas inteligentes recargables electrónicamente, las cuales almacenan o bien un saldo que se reduce cada vez que el usuario utiliza un medio de transporte o bien un bono multiviaje o un abono temporal. Las tarjetas inteligentes se recargan, por ejemplo, en terminales de recarga disponibles en las estaciones (de tren, de autobús, de metro, etc.), en quioscos, estancos, cajeros automáticos u otros establecimientos. Dichos terminales se encuentran habitualmente

comunicados con un servidor central, que a su vez se encuentra comunicado con una pasarela de pago, por ejemplo un sistema de pago por tarjeta de crédito. El usuario que desea recargar su tarjeta generalmente introduce la tarjeta inteligente a recargar y una tarjeta de crédito en el terminal de recarga, el cual obtiene datos de ambas tarjetas y solicita al servidor que gestione el pago de la recarga a través de la pasarela de pago; una vez realizado satisfactoriamente el pago y recibida una confirmación, el servidor ordena al terminal de recarga que efectúe una escritura en la memoria de la tarjeta inteligente reflejando la recarga del billete adquirido.

Un ejemplo de este tipo de sistema es el conocido como Barik®, utilizado en el sistema de transporte público de Bizkaia. Las tarjetas inteligentes comprendidas en el sistema Barik® incluyen el chip modelo MIFARE DESFire EV1 4K de NXP®, que se caracteriza por requerir unos procedimientos de seguridad especiales basados en claves secretas que se almacenan tanto en las tarjetas como en el terminal de recarga, en este último en un elemento de gran seguridad denominado módulo de seguridad SAM (“Secure Access Module” en inglés). Cuando se introduce una tarjeta inteligente del sistema Barik® en el terminal de recarga, el terminal de recarga realiza una autenticación entre dichas claves de seguridad almacenadas en la tarjeta y en el terminal de recarga. Se trata de una autenticación mutua de las claves de seguridad almacenadas tanto en la tarjeta inteligente como en el módulo de seguridad SAM del terminal de recarga. Como resultado de dicha autenticación mutua se genera una clave aleatoria o clave de sesión que se utiliza para cifrar una serie de datos intercambiados localmente entre la tarjeta inteligente y el terminal de recarga. La clave de sesión tiene una validez temporal, dejando de ser válida al separar o alejar físicamente la tarjeta inteligente del terminal de carga. Dicha separación entre la tarjeta inteligente y el terminal de carga provoca la desenergización del chip de la tarjeta inteligente y el fin de la sesión de recarga.

La presente invención tiene como objetivo proporcionar un sistema de gestión y recarga de billetes de transporte soportados en tarjetas inteligentes, donde no se requiera de terminales de recarga en estaciones

u otros establecimientos, y se reduzca por tanto el coste del fabricación, operación y mantenimiento del sistema.

Descripción breve de la invención

Es objeto de la presente invención un sistema de recarga de tarjetas inteligentes para su uso como billetes de transporte, que comprende un servidor, diversos terminales de usuario, y tarjetas inteligentes capaces de comunicarse con los terminales de usuario por medio de tecnología NFC (“Near Field Communication”, en inglés). El servidor comprende una unidad de procesado y una unidad de memoria comunicada con la unidad de procesado. Además, el servidor contiene al menos una clave de seguridad. Los terminales de usuario son terminales portátiles electrónicos inalámbricos dotados de tecnología NFC, y provistos de una unidad de procesado y una unidad de memoria comunicada con la unidad de procesado. La unidad de procesado del terminal de usuario puede establecer comunicación con la unidad de procesado del servidor a través de una red de comunicaciones electrónicas, tal como Internet. Las tarjetas inteligentes comprenden un chip pasivo provisto de una memoria con datos de la tarjeta inteligente.

La memoria del terminal de usuario almacena instrucciones para causar que la unidad de procesado del terminal de usuario realice al menos las operaciones siguientes: establecer una comunicación NFC inicial con la tarjeta inteligente para detectar la presencia de dicha tarjeta inteligente; establecer una comunicación remota con el servidor; actuar de intermediaria para el establecimiento de una autenticación mutua entre al menos una clave del chip de la tarjeta inteligente y al menos una clave de seguridad del servidor; recibir una verificación del servidor sobre el estado de la tarjeta inteligente; enviar una orden al servidor para que curse un pago a través de una plataforma de pago comunicada con el servidor; recibir una confirmación del servidor de que el pago ha sido realizado correctamente; establecer una comunicación NFC adicional con la tarjeta inteligente; escribir en la memoria del chip de la tarjeta inteligente información de una compra asociada al pago, comprendiendo normalmente dicha información un título de transporte recién adquirido y

pagado así como el correspondiente recibo o ticket del pago.

El sistema descrito presenta diversas ventajas. Por una parte, elimina la necesidad de costosos terminales de recarga en las estaciones de autobús, metro, etc., reduciendo el coste del mantenimiento del sistema. En su lugar, se posibilita que los usuarios puedan aprovechar su teléfono móvil para usarlo como terminal que recarga la tarjeta inteligente de transporte, aumentando enormemente la comodidad de uso para el usuario, que puede recargar la tarjeta en cualquier momento o lugar, sin necesidad de acudir físicamente a una estación, quiosco, cajero automático u otro establecimiento.

Además, en modos de realización preferentes, la autenticación de la tarjeta inteligente incluye el uso de claves almacenadas en la tarjeta inteligente y en el servidor, pero no en el terminal de usuario que efectúa la recarga. Dichos modos de realización proporcionan un sistema particularmente seguro y resistente a ataques informáticos a través de accesos indeseados a los terminales de usuario.

Descripción breve de las figuras

Los detalles de la invención se aprecian en las figuras que se acompañan, no pretendiendo éstas ser limitativas del alcance de la invención:

- La Figura 1 muestra un diagrama de bloques de un ejemplo de sistema de recarga de billetes de transporte en tarjetas inteligentes, de acuerdo con la presente invención.

Descripción detallada de la invención

La Figura 1 muestra un diagrama de bloques de un ejemplo de sistema (1) de recarga de tarjetas inteligentes distribuidas, para su uso como billetes de transporte, de acuerdo con la presente invención. Una serie de usuarios (99) del sistema (1) son portadores de una respectiva tarjeta inteligente (10), que puede ser recargada con facilidad mediante el

sistema (1) y puede ser utilizada como billete de transporte, por ejemplo en un sistema de transporte público.

El sistema (1) comprende un servidor (20) y una serie de terminales de usuario (30) portátiles electrónicos inalámbricos que son capaces de comunicarse remotamente con el servidor (20) a través de una red de comunicaciones electrónicas (40) tal como Internet, a la cual los terminales de usuario (30) se conectan por medio de una red de comunicaciones inalámbrica (41), como por ejemplo una red WIFI, GPRS, 3G, 4G, etc. El servidor (20) puede estar conectado a la red de comunicaciones electrónicas (40) de manera inalámbrica o alámbrica, no siendo ello relevante para la presente invención.

El servidor (20) comprende una unidad de procesado (21) y una unidad de memoria (22) comunicada con la unidad de procesado (21). Además el servidor (20) contiene al menos una clave de seguridad. En relación con las tarjetas inteligentes (10) distribuidas, el servidor únicamente almacena cierta información mínima, comprendiendo esencialmente dicha información mínima algún tipo de código identificativo de las tarjetas inteligentes y algún dato relativo al estado de dichas tarjetas inteligentes (10), residiendo los datos de las tarjetas inteligentes (10) en la propia tarjeta inteligente (10). Se entiende que el servidor (20) puede ser un único equipo, o varios equipos comunicados local o remotamente entre sí; idéntico razonamiento aplica a la unidad de procesado (21) y a la unidad de memoria (22) del servidor (20).

A su vez, los terminales de usuario (30) portátil inalámbricos comprenden una unidad de procesado (31) y una unidad de memoria (32) comunicada con la unidad de procesado (31). La unidad de procesado (31) y la unidad de memoria (32) albergan las instrucciones necesarias para que la unidad de procesado (31) del terminal de usuario (30) pueda establecer comunicación con la unidad de procesado (21) del servidor (20) a través de la citada red de comunicaciones electrónicas (40), por ejemplo sobre protocolos de comunicaciones de Internet. Además, la unidad de procesado (31) y la unidad de memoria (32) de los terminales de usuario (30) comprenden las

instrucciones necesarias para soportar la funcionalidad NFC (en inglés, “Near Field Communication”). El terminal de usuario (30) comprende además al menos un conjunto transmisor/receptor de radiofrecuencia (33) para comunicar inalámbricamente con la red de comunicaciones inalámbrica (41) y con las tarjetas inteligentes (10). En distintos modos de realización, el conjunto transmisor/receptor de radiofrecuencia (33) puede incluir uno o más transmisores, receptores, transmisores-receptores o transceptores de radiofrecuencia. La comunicación con las tarjetas inteligentes (10) tiene lugar mediante el protocolo NFC.

Por su parte, las tarjetas inteligentes (10) comprendidas en el sistema (1) incluyen un chip (11) provisto de una memoria (12) y de un transmisor-receptor de radiofrecuencia (13), o un transceptor de radiofrecuencia, en otros modos de realización. Un ejemplo no limitativo de chip (11) es el chip MIFARE DESFire EV1 4K de NXP® conocido en el mercado en la actualidad. El chip (11) de la tarjeta inteligente (10) es capaz de comunicarse inalámbricamente con un terminal de usuario (30) a través del transmisor-receptor de radiofrecuencia (13) y utilizando el protocolo NFC. La comunicación NFC puede establecerse, por ejemplo, en la banda de frecuencia de 13.56 MHz de acuerdo la norma 14443 y 18092 de NFC. Para establecer la comunicación NFC, el conjunto transmisor/receptor de radiofrecuencia (33) del terminal de usuario (30) emite una señal de radiofrecuencia que, al ser recibida por el transmisor-receptor de radiofrecuencia (13) del chip (11) de la tarjeta inteligente (10), produce la activación del chip (11). El chip (11) es pasivo, es decir, no se encuentra alimentado activamente por una batería u otra fuente de alimentación sino que es alimentado por señales de radiofrecuencia recibidas del exterior, de acuerdo con la tecnología NFC. El transmisor-receptor de radiofrecuencia (13) funciona por inducción electromagnética.

En un ejemplo de funcionamiento del sistema (1), un usuario (99) es portador de una tarjeta inteligente (10) que utiliza como billete de transporte público. La tarjeta inteligente (10) es capaz de almacenar al menos un título de transporte que puede ser un saldo, o un bono multiviaje, o un bono mensual de transporte, o un bono anual de transporte, o cualquier otra configuración de título de transporte, no

siendo dicha configuración relevante para la presente invención. Además, el usuario (99) es portador de un terminal de usuario (30) portátil inalámbrico, tal como un teléfono móvil de tipo “smartphone”, con capacidad procesadora y de almacenamiento suficiente como para albergar un sistema operativo que permita la descarga y ejecución de aplicaciones, generalmente a través de la red de comunicaciones electrónicas (40) y según se conoce en el estado del arte. El usuario (99) ha descargado e instalado en su terminal de usuario (30) una aplicación de sistema, la cual permite al terminal de usuario (30) ejecutar el método que se describe a continuación, y proporciona al usuario (99) un interfaz de usuario para la configuración y control de la ejecución del procedimiento; dicho interfaz de usuario puede ser gráfico, auditivo, táctil o una combinación de ellos.

Cuando el usuario (99) desea recargar la tarjeta inteligente (10) para poder ser utilizada para viajar, el usuario (99) accede en su terminal de usuario (30) a la aplicación del sistema, a través del interfaz de usuario de dicha aplicación, generándose una orden de iniciar una recarga. Opcionalmente, el usuario (99) ha podido registrarse previamente en el servidor (20).

Cuando la aplicación del sistema (1) (y por tanto, la unidad de procesado (31) del terminal de usuario (30) que se encuentra ejecutando dicha aplicación) detecta una orden de iniciar una recarga se implementa una fase de establecimiento de comunicaciones. Inicialmente establece una comunicación NFC con la tarjeta inteligente (10) para detectar la presencia de dicha tarjeta inteligente (10) y realizar una lectura de una serie de datos mínimos identificativos del tipo de tarjeta inteligente (10). Seguidamente, la aplicación establece una comunicación remota con el servidor (20) del sistema (1) para comprobar que el servidor (20) está activo, ya que en caso contrario no podrá ejecutarse el resto del procedimiento. En caso de existir conectividad con el servidor (20) se establece una autenticación mutua entre al menos una clave del chip (11) y al menos una clave de seguridad del servidor (20) y de forma que el terminal de usuario (30) no almacena ninguna clave propia ni tampoco lee ninguna clave de la tarjeta inteligente (10). La función del terminal de

usuario (30) es actuar de intermediario entre la tarjeta inteligente (10) y el servidor (20). Adicionalmente, la unidad de procesado del servidor (20) accede a la información mínima de la tarjeta inteligente (10) (código identificativo y estado) para verificar la existencia de la tarjeta inteligente (10) y su estado activo, chequeándose posibles situaciones fraudulentas o indeseadas. Posteriormente se genera una clave aleatoria o clave de sesión. En caso de no existir conectividad con el servidor (20), o bien en caso de fallar la autenticación mutua y no ser reconocida la tarjeta inteligente (10) por el servidor (20), o bien en caso de detectarse cualquier tipo de situación fraudulenta o indeseada, el proceso se da por concluido.

Realizadas con éxito las comprobaciones anteriores y generada la clave de sesión, puede procederse a la lectura de datos de la tarjeta inteligente (10) como se detalla a continuación. El servidor (20) elabora un paquete de datos cifrado mediante una clave de seguridad enviándose dicho paquete de datos cifrado al terminal de usuario (30). El terminal de usuario (30) no almacena ninguna clave asociada a ninguna tarjeta inteligente (10), de modo que no es capaz de descifrar el paquete de datos cifrado recibido y, en consecuencia, transmite el paquete de datos cifrado a la tarjeta inteligente (10). La tarjeta inteligente (10) en cambio, al contrario que el terminal de usuario (30) pero al igual que el servidor (20), sí almacena claves. Mediante la utilización de dichas claves, la tarjeta inteligente (10) desencripta el paquete de datos cifrado recibido y elabora un paquete cifrado posterior, conteniendo ya datos de la tarjeta inteligente (10) (como por ejemplo el saldo actual de la tarjeta inteligente (10)), enviándose este paquete cifrado posterior al servidor (20) a través del terminal de usuario (30). Finalmente el servidor (20), tras un adecuado control o verificación, envía los datos de la tarjeta inteligente (10) ya sin cifrar al terminal de usuario (30) y dichos datos son mostrados al usuario (99).

Es decir que, en la realización preferente del sistema (1) de acuerdo con la invención que se está describiendo, a excepción de cierta información mínima, como por ejemplo los códigos identificativos de las tarjetas inteligentes (10), cualquier dato de una tarjeta inteligente (10) se

transmite siempre de forma cifrada al servidor (20), a través del terminal de usuario (30), de modo que posteriormente el servidor (20) descifra dichos datos recibidos y los envía, ya de forma no cifrada, al terminal de usuario (30). Las claves utilizadas para el cifrado no viajan a través de las redes de comunicaciones (40, 41) ni tampoco son almacenadas en el terminal de usuario (30).

De forma opcional, la autenticación mutua entre las claves de chip (11) y las claves del servidor (20) y la generación de la clave de sesión puede establecerse mediante las operaciones que se describen a continuación. En la fase de establecimiento de las comunicaciones, se genera al menos un número aleatorio cifrado a partir de al menos una clave del chip (11) de la tarjeta inteligente (10). Dicho número aleatorio cifrado con la clave del chip (11) es transmitido al servidor (20). El servidor (20) comprende un Módulo de Acceso Seguro (SAM) que procesa el número aleatorio cifrado recibido y genera una clave de sesión. Dicha clave de sesión se utiliza para el cifrado de datos de la tarjeta inteligente (10), transmitidos al servidor (20) a través del terminal de usuario (30) para su posterior control. El terminal de usuario (30) carece por tanto de Módulo de Acceso Seguro (SAM) y únicamente tiene acceso a datos cifrados, realizando un intercambio remoto de dichos datos cifrados entre la tarjeta inteligente (10) y el servidor (20). El hecho de que el terminal de usuario (30) no pueda descifrar los datos cifrados intercambiados, puesto que no almacena las correspondientes claves, aumenta de forma altamente ventajosa la seguridad del sistema (1) contra, por ejemplo, posibles ataques informáticos.

Por otra parte, la clave de sesión generada de forma remota con la intervención del servidor (20), por el procedimiento anteriormente expuesto, es una clave temporal, variable o volátil en el sentido de que deja de ser válida en caso de interrumpirse la comunicación entre la tarjeta inteligente (10) y el terminal de usuario (30). En dicho caso, el sistema (1) permite implementar un nuevo proceso de establecimiento de comunicaciones, comprobaciones de seguridad y generación de una nueva clave de sesión.

Establecida la sesión, el usuario (99) podrá definir las características de un título de transporte que pretende comprar o adquirir. Así, la aplicación puede dar a elegir al usuario (99) el tipo de título de transporte con el que se desea cargar la tarjeta, tal como un saldo para realizar viajes individuales, un bono semanal, un bono mensual, un bono anual, etc. Alternativamente, la aplicación puede seleccionar el mismo tipo de título con el que el usuario (99) haya realizado la recarga anterior.

Entonces, la aplicación envía una orden al servidor (20) para que curse un pago a través de una plataforma de pago (50) comunicada con el servidor (20). La plataforma de pago (50) puede ser, por ejemplo, una entidad financiera de pago por tarjeta de crédito, un sistema de pago online tal como PayPal®, etc., no siendo el tipo de plataforma de pago (50) relevante para la presente invención. El servidor (20) indica a la plataforma de pago (50) el importe del pago así como la cuenta de usuario, cuenta bancaria, tarjeta de crédito u otra cuenta asociada con el usuario (99) a la que se debe cargar el pago.

Una vez que la plataforma de pago (50) ha tramitado el pago con éxito, envía una señal de confirmación al servidor (20), el cual envía a su vez una señal de confirmación de pago a la unidad de procesado (31) del terminal de usuario (30) portátil inalámbrico. La unidad de procesado (31) recibe dicha señal de confirmación de pago del servidor (20), y presenta al usuario una indicación de que aproxime la tarjeta inteligente (10) al terminal de usuario (30). La indicación puede consistir, por ejemplo, en un mensaje mostrado en una pantalla (34) del terminal de usuario (30) o emitiendo un mensaje auditivo a través de un altavoz (no representado) tal como “Coloque su teléfono sobre su tarjeta”.

La información asociada a la compra del título de transporte adquirido cuyo pago acaba de realizarse con éxito es transmitida por el servidor (20) a unidad de procesado (31) del terminal de usuario (30). Finalmente, el terminal de usuario (30) emite una orden de escritura, dirigida al chip (11) de la tarjeta inteligente (10), con la información asociada al título de transporte. En consecuencia, el conjunto transmisor/receptor de radiofrecuencia (33) del terminal de usuario (30)

emite una señal NFC de escritura conteniendo dicha información asociada al título de transporte. El transmisor-receptor de radiofrecuencia (13) de la tarjeta inteligente (10) recibe dicha señal NFC de escritura y, seguidamente, la información contenida en dicha señal NFC de escritura es escrita en la memoria (12) del chip (11) de la tarjeta inteligente (10). Dicha información puede comprender, por ejemplo, un dato numérico correspondiente a un saldo monetario. Alternativa o adicionalmente, dicha información puede comprender información relativa a un periodo de tiempo de validez de un título de transporte; por ejemplo, dicha información puede comprender información relativa a un periodo de validez de un saldo, o información relativa a un periodo de validez de un título de transporte (por ejemplo, mes de Agosto del año 2015).

En algunos modos de realización, puede intercambiarse información adicional cifrada entre el chip (11) de la tarjeta inteligente (10) y el servidor (20), de forma que el servidor (20) puede descifrar y enviar al terminal de usuario (30) datos de la tarjeta inteligente (10) tales como fecha de caducidad, datos del titular, saldo, movimientos recientes, recargas recientes, utilizaciones recientes, validación de viajes, etc.

Se contemplan realizaciones de la invención en las cuales el sistema (1) permite realizar otras operaciones sobre la tarjeta inteligente (10) tales como modificaciones de la fecha de caducidad u otras.

En resumen, el sistema (1) descrito permite que los usuarios puedan aprovechar su teléfono móvil con funcionalidad NFC para usarlo con total seguridad como un terminal de recarga de una tarjeta inteligente de transporte. Basta que el usuario se descargue una aplicación del sistema para que el móvil pueda establecer comunicación entre el servidor del sistema y la tarjeta inteligente, gestionar una compra y transferir un título de transporte a la tarjeta inteligente, todo ello de manera segura a pesar de que se utilice un dispositivo no necesariamente seguro (el teléfono móvil) y un canal de comunicación no necesariamente seguro (Internet), gracias a que los elementos de los extremos (la tarjeta inteligente y el servidor) albergan las claves involucradas en el proceso.

Los paquetes de datos viajan entre la tarjeta inteligente y el servidor de forma cifrada. Las claves utilizadas para dicho cifrado no viajan a través del canal de comunicación ni son almacenadas en el dispositivo utilizado como terminal.

REIVINDICACIONES

1. Sistema (1) de recarga de tarjetas inteligentes para su uso como billetes de transporte, que se caracteriza por que comprende:

- un servidor (20), que comprende una unidad de procesado (21) y una unidad de memoria (22) comunicada con la unidad de procesado (21);

- al menos un terminal de usuario (30) portátil inalámbrico dotado de tecnología NFC, donde dicho terminal de usuario (30) comprende una unidad de procesado (31) y una unidad de memoria (32) comunicada con la unidad de procesado (31), y donde dicha unidad de procesado (31) del terminal de usuario (30) puede establecer comunicación con la unidad de procesado (21) del servidor (20) a través de una red de comunicaciones electrónicas (40);

- al menos una tarjeta inteligente (10), que comprende un chip (11) provisto de una memoria (12) con datos de la tarjeta inteligente (10); donde

- la unidad de memoria (32) del terminal de usuario (30) almacena instrucciones para:

  - establecer una comunicación NFC inicial entre la unidad de procesado (31) y la tarjeta inteligente (10) para detectar la presencia de dicha tarjeta inteligente (10);
  - establecer una comunicación remota entre la unidad de procesado (31) y el servidor (20);
  - intercambiar datos cifrados entre la tarjeta inteligente (10) y el servidor (20);
  - recibir en la unidad de procesado (31) una verificación del servidor (20) sobre el estado de la tarjeta inteligente (10);
  - enviar desde la unidad de procesado (31) una orden al

servidor (20) para que curse un pago a través de una plataforma de pago comunicada con el servidor (20);

- recibir en la unidad de procesado (31) una confirmación del servidor (20) de que el pago ha sido realizado correctamente;
- establecer una comunicación NFC adicional entre la unidad de procesado (31) y la tarjeta inteligente (10);
- escribir en la memoria (12) del chip (11) de la tarjeta inteligente (10) información de una compra asociada al pago.

2. Sistema (1), según la reivindicación 1, que se caracteriza por que el servidor (20) comprende un Módulo de Acceso Seguro (SAM) generador de una clave de sesión para el cifrado de datos de la tarjeta inteligente (10).

3. Sistema (1), según la reivindicación 1, que se caracteriza por que el terminal de usuario (30) es un terminal que se encuentra comunicado con la red de comunicaciones electrónicas (40) a través de una red de comunicaciones inalámbrica (41).

4. Sistema (1), según la reivindicación 3, que se caracteriza por que el terminal de usuario (30) es un teléfono móvil.

5. Sistema (1), según la reivindicación 1, que se caracteriza por que la información de la compra asociada al pago comprende al menos un dato numérico correspondiente a un saldo, a un título de transporte, a un bono multiviaje o a un abono temporal.

6. Método de recarga de tarjetas inteligentes para su uso como billetes de transporte que se caracteriza por que comprende los pasos de:

- disponer de un servidor (20), de al menos un terminal de usuario (30) portátil inalámbrico dotado de tecnología NFC y de al menos una tarjeta inteligente (10) que comprende un chip (11) provisto de una memoria (12) con datos de la tarjeta

inteligente (10);

- establecer una comunicación NFC inicial entre el terminal de usuario (30) y la tarjeta inteligente (10) para detectar la presencia de dicha tarjeta inteligente (10);
- establecer una comunicación remota entre el terminal de usuario (30) y el servidor (20) a través de una red de comunicaciones electrónicas (40), donde dicho servidor (20) contiene al menos una clave de seguridad;
- utilizar terminal de usuario (30) como intermediario para establecer una autenticación mutua entre al menos una clave del chip (11) de la tarjeta inteligente (10) y al menos una clave de seguridad del servidor (20);
- enviar desde el terminal de usuario (30) una orden al servidor (20) para que curse un pago a través de una plataforma de pago comunicada con el servidor (20);
- recibir en el terminal de usuario (30) una confirmación del servidor (20) de que el pago ha sido realizado correctamente;
- establecer una comunicación NFC adicional entre el terminal de usuario (30) y la tarjeta inteligente (10);
- escribir en la memoria (12) del chip (11) de la tarjeta inteligente (10) información de una compra asociada al pago.

7. Método, según la reivindicación 6, que se caracteriza por que el establecimiento de la autenticación mutua comprende los pasos adicionales de:

- generar al menos un número aleatorio cifrado a partir de al menos una clave del chip (11) de la tarjeta inteligente (10),
- enviar dicho número aleatorio a un Módulo de Acceso Seguro (SAM) del servidor (20) para la generación de una clave de sesión a partir del procesamiento del número aleatorio, donde dicha clave de sesión se utiliza para cifrar datos de la tarjeta inteligente (10).

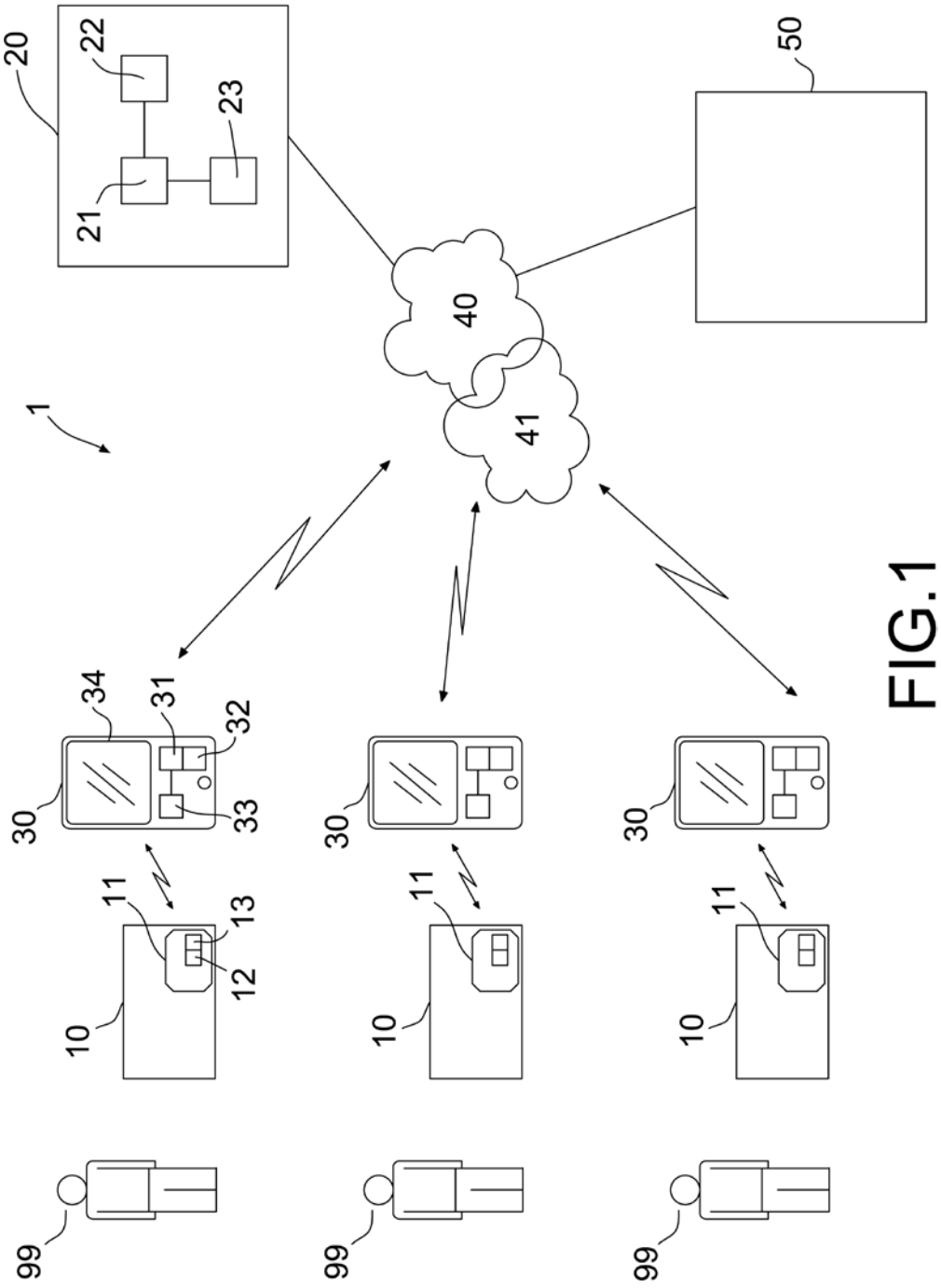

FIG.1

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201531014

(22) Fecha de presentación de la solicitud: 10.07.2015

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

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

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2014019216 A1 (JO BYUNG YONG) 16.01.2014, párrafos [0003],[0005],[0008],[0047-0048],[0057-0059],[0061]; reivindicación 10; figuras 3-6.	1-7
A	US 2012130838 A1 (KOH LIANG SENG et al.) 24.05.2012, todo el documento.	1-7
A	WO 2011006414 A1 (ZTE CORP et al.) 20.01.2011, todo el documento.	1-7
A	US 2014006194 A1 (XIE XIANGZHEN et al.) 02.01.2014, todo el documento.	1-7

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**
29.04.2016	D. Cavia del Olmo	1/4

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

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

Fecha de Realización de la Opinión Escrita: 29.04.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	7	**SI**
	Reivindicaciones	1-6	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-7	**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	US 2014019216 A1 (JO BYUNG YONG)	16.01.2014
D02	US 2012130838 A1 (KOH LIANG SENG et al.)	24.05.2012
D03	WO 2011006414 A1 (ZTE CORP et al.)	20.01.2011
D04	US 2014006194 A1 (XIE XIANGZHEN et al.)	02.01.2014

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 del estado de la técnica más próximo al objeto de la solicitud reivindicado. Siguiendo la redacción de la reivindicación independiente, D01 describe un sistema de pago de billetes de transporte mediante tarjetas inteligentes recargables (ver título y párrafos [0003] y [0005]) caracterizado, entre otros, por los siguientes elementos técnicos:
- Un servidor (ver referencia 310 en figuras 3 y 6).
- Un elemento de pago o terminal de usuario que, en una de las posibles realizaciones puede ser un teléfono móvil que puede estar dotado de tecnología NFC (ver párrafos [0047-0048]) y dispone de un procesador (ver figura 7) que establece comunicación con el servidor a través de una red de comunicaciones inalámbricas.
- Al menos una tarjeta inteligente dotada de tecnología NFC y medios para el almacenamiento de los datos relativos a la tarjeta (ver párrafo [0008]).

El terminal de usuario establece comunicación NFC con la tarjeta inteligente detectando así su presencia (ver referencias 330 y 340 en figura 3 y párrafos [0047] y [0048]).
En D01 se describen dos realizaciones posibles para la realización del pago o recarga de la tarjeta: en una de ellas, tal y como se reivindica en R1, el dispositivo de pago (o teléfono móvil) no dispone de Módulo de Acceso Seguro (SAM) y se limita a realizar el intercambio remoto de dichos datos entre la tarjeta inteligente y el servidor (ver etapa 430 en figura 4 y párrafo [0059]) estableciendo de este modo la validez de los medios de pago asociados a la tarjeta.
A continuación (ver etapa 445 en figura 4, figura 3 y párrafo [0061]), desde el dispositivo móvil se envía orden al servidor para que curse el pago correspondiente y se verifica la validez de los medios de pago mediante un Módulo de Acceso Seguro (SAM) a través del servidor (ver reivindicación 10).
La comunicación establecida entre el terminal de usuario y la tarjeta inteligente es de lectura/escritura y bidireccional (ver párrafo [0057]).
En relación a la reivindicación independiente de producto R1, y teniendo en cuenta en contenido de D01, se concluye que R1 carece de novedad en el sentido del artículo 6.1 de la Ley de Patentes puesto que las características técnicas reivindicadas en R1 aparecen descritas de forma explícita o implícita en D01 donde desarrollan la misma función técnica.
Las reivindicaciones dependientes R2, R3, R4 y R5 carecen de novedad del mismo modo que la reivindicación independiente de la cual dependen; las características técnicas reivindicadas en R2, R3 y R4 se encuentran descritas en D01 mientras que las características técnicas reivindicadas en R5, a pesar de que no se encuentran explícitamente descritas en D01, se consideran características técnicas implícitas.
Por lo que respecta a la reivindicación independiente de procedimiento R6, se considera D01 el documento más próximo dentro del estado de la técnica. Siguiendo la redacción de R6, D01 describe un método de uso y recarga de tarjetas inteligentes para su uso como billetes de transporte que se caracteriza, entre otras, por las siguientes etapas:
- Disponer de un servidor, un terminal de usuario portátil inalámbrico dotado de tecnología NFC y de al menos una tarjeta inteligente que comprende un chip provisto de una memoria con datos de la tarjeta inteligente.
- Establecer una comunicación NFC inicial entre el terminal de usuario y la tarjeta inteligente para detectar la presencia de dicha tarjeta.
- Establecer una comunicación remota entre el terminal de usuario y la tarjeta inteligente detectando así la presencia de dicha tarjeta inteligente.
- Establecer comunicación remota entre el terminal de usuario y el servidor a través de una red de comunicaciones electrónicas.
- Enviar desde el dispositivo móvil orden al servidor para que curse el pago correspondiente y se verifica la validez de los medios de pago a través de un Módulo de Acceso Seguro (SAM) a través del servidor (ver reivindicación 10).
- La comunicación establecida entre el terminal de usuario y la tarjeta inteligente es de lectura/escritura y bidireccional (ver párrafo [0057]).

En relación a la reivindicación independiente de procedimiento R6, y a la vista del contenido de D01, se considera que R6 carece de novedad en el sentido del artículo 6.1 de la Ley de Patentes según razonamiento análogo al planteado para R1.
Por lo que respecta a la reivindicación dependiente de procedimiento R7, ésta carece de actividad inventiva en el sentido del artículo 8.1 de la Ley de Patentes puesto que se considera que las características técnicas que reivindica constituyen una variante constructiva que el experto en la materia se plantearía para el caso en cuestión sin la aplicación de actividad inventiva. Para ilustrar este punto, se recomienda la lectura del documento D02 perteneciente al mismo campo técnico (ver párrafos [0073] y [0126]).
Los documentos D03 y D04 son representativos dentro del estado de la técnica y se recomienda su lectura.