(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 739 206**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 12/08 (2009.01)
G06Q 20/32 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.08.2017 E 17185122 (3)**

(97) Fecha y número de publicación de la concesión europea: **22.05.2019 EP 3442249**

(54) Título: **Método para prevenir el uso no autorizado de autorizaciones de acceso electrónico que se pueden gestionar en dispositivos móviles electrónicos por medio de una aplicación de cartera, pudiéndose transferir a los dispositivos electrónicos móviles desde un servidor por medio de un enlace para la descarga de las autorizaciones de acceso**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.01.2020

(73) Titular/es:

SKIDATA AG (100.0%)
Untersbergstrasse 40
5083 Grödig/Salzburg, AT

(72) Inventor/es:

MALMBORG, ANDERS y
JAYAPRAKASH, VAIJAYANTHI MALA

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

DESCRIPCIÓN

Método para prevenir el uso no autorizado de autorizaciones de acceso electrónico que se pueden gestionar en dispositivos móviles electrónicos por medio de una aplicación de cartera, pudiéndose transferir a los dispositivos electrónicos móviles desde un servidor por medio de un enlace para la descarga de las autorizaciones de acceso

[0001] La presente invención se refiere a un método para prevenir el abuso de dispositivos móviles electrónicos por medio de una aplicación de cartera de autorizaciones de acceso, las cuales se proporcionan a los dispositivos electrónicos móviles desde un servidor por medio de un respectivo enlace para la transmisión de la autorización de acceso, de acuerdo con el preámbulo de la reivindicación 1.

[0002] En la técnica anterior se describen autorizaciones de acceso electrónico, por ejemplo mediante el almacenamiento y administración de las llamadas aplicaciones de cartera en dispositivos electrónicos móviles, tales como en teléfonos inteligentes, y los tablet. En este caso, es posible enviar autorizaciones de acceso electrónico a otros dispositivos electrónicos móviles, por ejemplo, a través de la aplicación "Wallet" de IOS. Por un lado, esto aumenta la comodidad en caso de que una persona autorizada desee utilizar un nuevo dispositivo electrónico móvil; por otro lado, las autorizaciones personales de acceso electrónico pueden, por lo tanto, ser "prestadas", como resultado de lo cual estas autorizaciones de acceso pueden ser objeto de un uso ilícito.

[0003] US 2016/350547 A1 da a conocer un método para evitar el mal uso mediante autorizaciones de acceso electrónico obtenidas mediante la interacción con un servidor, las cuales se transmiten desde el servidor a los dispositivos electrónicos móviles, con lo cual, tras la adquisición de la autorización de acceso electrónico por un comprador, se facilitan datos de autenticación y un dispositivo electrónico móvil, a los que la autorización de acceso electrónico es transmitida por el servidor, por lo que se transmite al servidor una ID individual del dispositivo electrónico móvil, que tiene una ID de la autorización de acceso adquirida, con lo que una transferencia de la autorización de acceso electrónico del dispositivo electrónico móvil a otro dispositivo electrónico se realiza solo después de la introducción de los datos de autenticación especificados por el comprador de la autorización de acceso mediante una interacción con el servidor. En el servidor, la ID de autorización de acceso está vinculada a la ID del dispositivo electrónico móvil adicional y la autorización de acceso marcada en el dispositivo electrónico móvil está marcada como no válida por el servidor.

[0004] La presente invención tiene por objeto proporcionar un método para prevenir el abuso de dispositivos electrónicos móviles por medio de una aplicación de cartera de autorizaciones de acceso electrónico, pudiéndose transferir a los dispositivos electrónicos móviles desde un servidor por medio de un enlace para la descarga de las autorizaciones de acceso, en cuya ejecución se proporcionará un uso indebido de una autorización de acceso condicional, al tiempo que se garantiza la posibilidad de transferir la autorización de acceso electrónico a otro dispositivo electrónico móvil de una persona autorizada.

[0005] Este objeto se resuelve mediante las características de la reivindicación 1. Otras realizaciones y ventajas según la invención emergen de las reivindicaciones secundarias.

[0006] En consecuencia, se propone un método para evitar el uso indebido de las autorizaciones de acceso electrónico manejables en dispositivos electrónicos móviles mediante una aplicación de cartera, que se transmiten a los dispositivos electrónicos móviles mediante un servidor mediante un enlace respectivo para descargar la autorización de acceso, en el curso del cual se adquiere una autorización de acceso electrónico mediante una interacción con un servidor, mediante la cual, al adquirir un comprador la autorización de acceso electrónico, se obtiene una contraseña o datos de autenticación y un dispositivo electrónico móvil al cual se transmite la autorización de acceso electrónico del servidor mediante un enlace para descargar la autorización de acceso.

[0007] Según la invención, se transmite una ID única del dispositivo electrónico móvil al servidor cuando se activa el enlace para la descarga de la autorización de acceso adquirida, la cual se asocia con una ID de la autorización de acceso adquirida, teniendo lugar una transmisión de la autorización de acceso electrónico del primer dispositivo electrónico móvil a otro dispositivo electrónico móvil solo después de ingresar la contraseña especificada por el comprador de la autorización de acceso o los datos de autenticación especificados por el comprador de la autorización de acceso mediante una interacción con el servidor, en donde tras la transmisión exitosa en el servidor, la ID de autorización de acceso se vincula con la ID del dispositivo electrónico móvil adicional, y el servidor marca la autorización de acceso almacenada en el primer dispositivo electrónico móvil como no válida.

[0008] De acuerdo con la invención, después de la comunicación del enlace para la descarga de la autorización de acceso al dispositivo electrónico móvil desde una aplicación de cartera que se instala en el dispositivo móvil, el enlace se ejecuta, y, para la descarga de la autorización de acceso adquirida, transmite una ID única del dispositivo electrónico móvil al servidor, con lo que se verifica en el servidor si una ID de la autorización de acceso adquirida está vinculada a la ID única transmitida del dispositivo electrónico móvil. Si este no es el caso, la ID de autorización de acceso y la ID única del dispositivo electrónico móvil están vinculadas entre sí y, a continuación, se descarga la autorización de acceso electrónico.

[0009] En el caso de que la autorización de acceso electrónico se transfiera de un dispositivo electrónico móvil a otro dispositivo electrónico móvil, la aplicación de cartera del dispositivo electrónico móvil, con cuya ID está vinculada la ID de autorización de acceso, transmite un enlace para descargar la autorización de acceso al dispositivo electrónico móvil adicional, en donde la aplicación de cartera del dispositivo electrónico móvil adicional ejecuta el enlace y transmite una ID única del dispositivo electrónico móvil adicional al servidor.

[0010] Según la invención, se verifica en el servidor si existe una conexión de ID de autorización de acceso con una ID única de otro dispositivo electrónico móvil, en el que, si este es el caso, el servidor transmite un enlace al otro dispositivo electrónico móvil, cuya ejecución desde la aplicación virtual conduce a una máscara de entrada para la contraseña especificada por el comprador de la autorización de acceso o los datos de autenticación especificados por el comprador de la autorización de acceso, en donde, en el caso de una contraseña válida o datos de autenticación válidos, la ID de autorización de acceso en el servidor se conecta con la ID del otro dispositivo electrónico móvil y la autorización de acceso electrónico se descarga en el dispositivo electrónico móvil adicional.

[0011] La autorización de acceso almacenada en el primer dispositivo electrónico móvil es marcada como no válida por el servidor, preferiblemente por medio de un mensaje de inserción a la aplicación de cartera, en donde el enlace entre la ID del primer dispositivo electrónico móvil se elimina con la autorización de acceso electrónico y los datos correspondientes se almacenan en el servidor.

[0012] De acuerdo con la concepción según la invención se describe un método para la prevención del abuso de dispositivos electrónicos móviles por medio de una aplicación de cartera de autorizaciones de acceso electrónico, con la descarga para los dispositivos electrónicos móviles desde un servidor por medio de uno de los enlaces del fabricante. De esta manera, se garantiza que la autorización de acceso solo se puede transferir a otro dispositivo electrónico móvil, si se trata de un dispositivo electrónico electrónico de una persona autorizada.

[0013] En el contexto de la invención, cuando ha de ser transmitida una autorización de acceso de un dispositivo electrónico móvil a otro dispositivo electrónico móvil, es decir, cuando la ID de autorización de acceso ya está conectada con una ID única de un dispositivo electrónico móvil, en base al número de conexiones logradas de la ID de autorización de acceso con la ID única de dispositivos electrónicos móviles, y la frecuencia con la que se verifica la autorización de acceso ya transmitida, por lo que, cuándo el número de transmisiones logradas ha alcanzado un umbral predeterminado, no es posible ninguna otra transmisión.

[0014] A continuación, la invención se describirá en más detalle, a modo de ejemplo, con referencia a la figura adjunta, la cual muestra un diagrama de secuencia para una ilustración de las características principales del método de la invención.

[0015] Haciendo referencia a la figura adjunta, en el inicio del proceso se adquiere una autorización de acceso electrónico por un comprador 1 por medio de una interacción con un servidor 2 (etapa 1), en donde se facilita una contraseña o información de autenticación con la adquisición de la autorización de acceso electrónico por el comprador. Posteriormente (paso 2), la autorización de acceso electrónico se transmite desde el servidor 1 a un dispositivo electrónico móvil 3 especificado tras la adquisición de la autorización de acceso por medio de un enlace para descargar la autorización de acceso, en donde una aplicación de cartera almacenada en el dispositivo móvil 3 está instalado, se ejecuta el enlace y se descarga la autorización de acceso adquirida. Una ID individual del dispositivo electrónico móvil al servidor 2 (paso 3), en el servidor 2 verifica si está conectada una ID de la autorización de acceso adquirida con la ID individualizada transmitida. Si esto no es el caso, se conectan entre sí la ID de autorización de acceso y la ID única del dispositivo electrónico móvil 3 (paso 4) y, a continuación, se descarga la autorización de acceso electrónico.

[0016] Si la autorización de acceso electrónico se transmite desde un dispositivo electrónico móvil 3 a otro dispositivo electrónico móvil 4, es decir, si la ID de autorización de acceso ya está vinculada a una ID única de un dispositivo electrónico móvil 3, después del inicio del procedimiento del propietario del dispositivo electrónico móvil 3 (paso 5), cuya ID única está vinculada a la ID de autorización de acceso, de la aplicación de cartera del dispositivo electrónico electrónico 3, con cuya ID única está vinculada la ID de autorización de acceso, se descarga de la autorización de acceso al otro dispositivo electrónico móvil 4 (paso 6), en donde la aplicación de cartera del otro dispositivo electrónico móvil 4 ejecuta el enlace (paso 7) y se transfiere una ID única del otro dispositivo electrónico móvil 4 al servidor 2.

[0017] Posteriormente, se comprueba en el servidor 2 si existe una conexión de la ID de la autorización de acceso transmitida con una ID única de otro dispositivo electrónico móvil, y si este es el caso, se transfiere un enlace desde el servidor 2 al otro dispositivo electrónico móvil 4 (paso 8), cuya ejecución conduce desde la aplicación de cartera a una máscara de entrada para la contraseña especificada por el comprador de la autorización de acceso o los datos de autenticación especificados por el comprador de la autorización de acceso (paso 9), por lo que la contraseña válida o datos de autenticación válidos, en el servidor 2 la ID de autorización de acceso está conectada con la ID del otro dispositivo electrónico móvil 4 (paso 10) y la autorización de acceso electrónico se descarga al otro dispositivo electrónico móvil 4.

[0018] A continuación, desde el servidor 2 en la aplicación de cartera se marca como no válida la autorización de

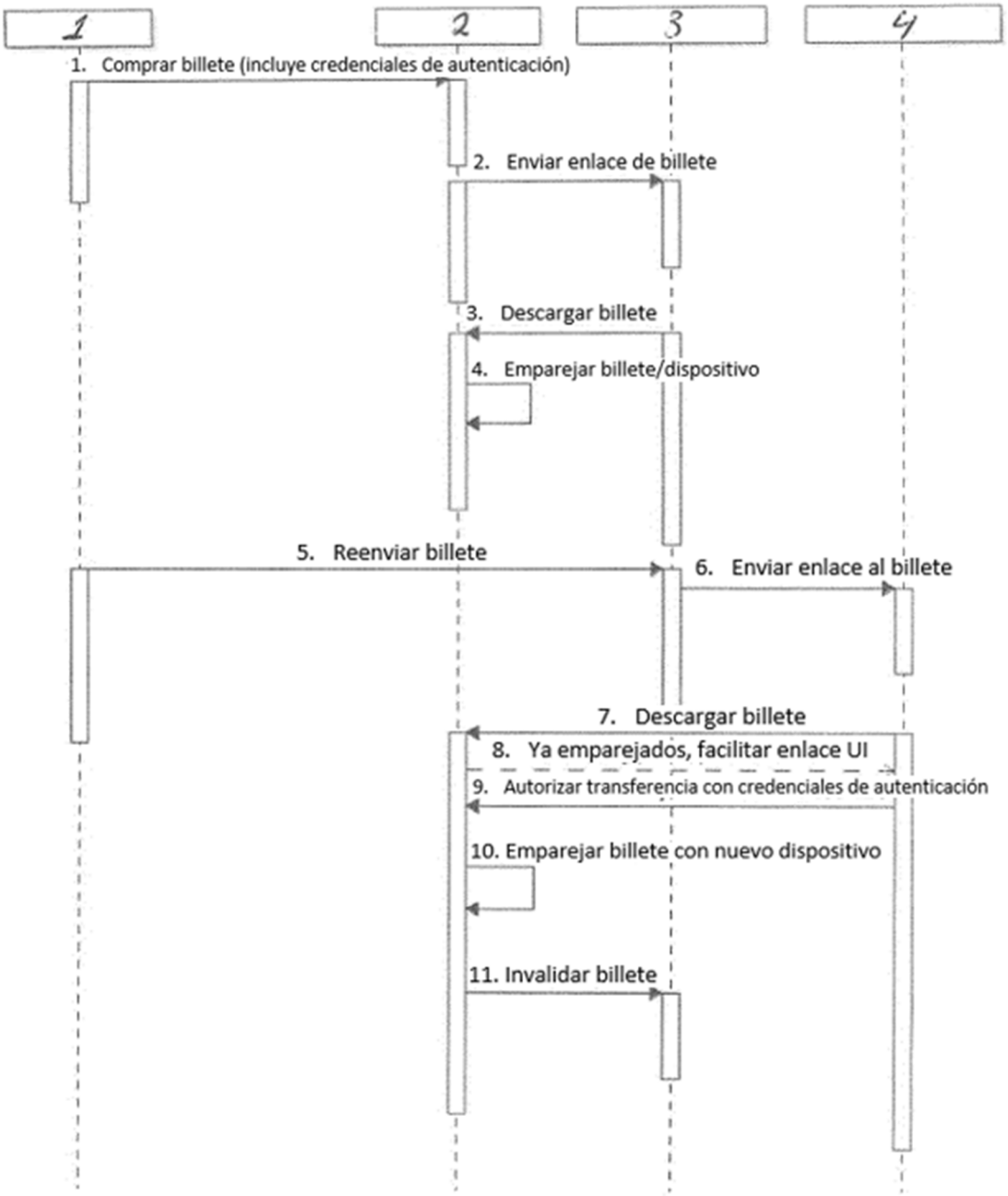
acceso almacenada en el primer dispositivo electrónico móvil 3 preferiblemente por medio de un mensaje de inserción (etapa 11).

REIVINDICACIONES

1. Un método para evitar el uso no autorizado de las autorizaciones de acceso electrónico que pueden gestionarse en dispositivos electrónicos móviles mediante una aplicación de cartera, que se transfieren a los dispositivos electrónicos móviles desde un servidor mediante un enlace para descargar la respectiva autorización de acceso, en donde una autorización de acceso electrónico se adquiere por medio de una interacción con el servidor (2), en donde durante la compra de la autorización de acceso electrónico una contraseña o datos de autenticación y un dispositivo electrónico móvil, para el cual la autorización de acceso electrónico se transfiere desde el servidor (2) por medio de un enlace para descargar la autorización de acceso, se indica por un comprador (1), donde, en una ID única del dispositivo electrónico móvil (3), se transfiere al servidor (2) durante la ejecución del enlace para descargar la autorización de acceso adquirida, asociándose dicha ID de dispositivo única con una ID de la autorización de acceso adquirida, en donde la transferencia de la autorización de acceso electrónico del dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4) solo se realiza después de la entrada mediante una interacción con el servidor (2) de la contraseña indicada por el comprador de la autorización de acceso. y/o de los datos de autenticación indicados por el comprador de la autorización de acceso, en donde, una vez completada la transferencia, la ID de autorización de acceso está asociada con la ID del otro dispositivo electrónico móvil (4) en el servidor (2) y la autorización de acceso en el archivo para el dispositivo móvil electrónico (3) está marcada como no válida por el servidor (2), en la que, después de la transferencia completa al dispositivo electrónico móvil (3) del enlace para descargar la autorización de acceso, la aplicación de cartera instalada en el dispositivo móvil (3) ejecuta el enlace y transfiere una ID única del dispositivo electrónico móvil al servidor (2) para descargar la autorización de acceso adquirida, en donde el servidor (2) revisa si una ID de la autorización de acceso adquirida está asociada con la ID única transferida del dispositivo electrónico móvil (3), en donde, si este no es el caso, la autorización de acceso ID y la ID única del dispositivo electrónico móvil (3) están asociadas entre sí y, posteriormente, se descarga la autorización de acceso electrónico y, si se pretende transferir una autorización de acceso electrónico desde un dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4), la aplicación de cartera del dispositivo electrónico móvil (3), cuya ID única está asociada con la ID de autorización de acceso, transfiere un enlace para descargar la autorización de acceso al otro dispositivo electrónico móvil (4) después de que el propietario del dispositivo electrónico móvil (3) haya iniciado este proceso, cuya ID exclusiva esté asociada a la ID de autorización de acceso, en la que se aplique la cartera del otro dispositivo electrónico móvil. El dispositivo (4) ejecuta el enlace y transfiere una ID única del otro dispositivo electrónico móvil (4) al servidor (2), en el que el servidor (2) revisa posteriormente si existe una asociación entre el ID de la autorización de acceso para ser transferida y una ID única de otro dispositivo electrónico móvil, en donde, si este es el caso, el servidor (2) transfiere un enlace al otro dispositivo electrónico móvil (4), la ejecución de dicho enlace resulta en un pantalla de entrada provista por la aplicación de cartera para ingresar la contraseña indicada por el comprador de la autorización de acceso y/o los datos de autenticación indicados por el comprador de la autorización de acceso, en donde, al ingresar una contraseña válida o una autenticación auténtica en los datos, la ID de autorización de acceso está asociada con la ID única del otro dispositivo electrónico móvil (4) en el servidor (2) y la autorización de acceso electrónico se descarga al otro dispositivo electrónico (4) y el acceso. La autorización archivada en el dispositivo electrónico móvil (3) está marcada como no válida, en donde la asociación de la ID única del dispositivo electrónico móvil (3) con la autorización de acceso electrónico se elimina y los datos respectivos se almacenan en el servidor (2). .

2. El método para evitar el uso no autorizado de autorizaciones de acceso electrónico que se pueden gestionar en dispositivos electrónicos móviles mediante una aplicación de cartera, que se transfieren a los dispositivos electrónicos móviles desde un servidor mediante un enlace para la descarga de la respectiva autorización de acceso, según la reivindicación 1, **caracterizándose porque**, si se pretende que una autorización de acceso se transfiera de un dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4), es decir, si la ID de autorización de acceso ya está asociada con una ID única de un dispositivo electrónico móvil (3), se realiza una revisión en función del número de asociaciones completadas de la ID de autorización de acceso con las ID únicas de los dispositivos electrónicos móviles, con qué frecuencia la autorización de acceso ya se ha transferido, en donde, si el número de transferencias completadas ha alcanzado un umbral definido, no es posible realizar más transferencias.

3. El método para evitar el uso no autorizado de autorizaciones de acceso electrónico que pueden administrarse en dispositivos electrónicos móviles mediante una aplicación de cartera, que se transfieren a los dispositivos electrónicos móviles desde un servidor mediante un enlace para la descarga de la respectiva autorización de acceso, según la reivindicación 1 o 2, caracterizándose porque, en el caso de una transferencia completa de la autorización de acceso electrónico del dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4), la autorización de acceso archivada en el dispositivo electrónico móvil (3) está marcada como no válida por el servidor (2) mediante un mensaje de inserción.


1
2
3
4
1. Comprar billete (incluye credenciales de autenticación)
2. Enviar enlace de billete
3. Descargar billete
4. Emparejar billete/dispositivo
5. Reenviar billete
6. Enviar enlace al billete
7. Descargar billete
8. Ya emparejados, facilitar enlace UI
9. Autorizar transferencia con credenciales de autenticación
10. Emparejar billete con nuevo dispositivo
11. Invalidar billete