(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 981 811**

(51) Int. Cl.:

G06Q 10/02	(2012.01)	***H04L 9/40***	(2012.01)
G06F 21/31	(2013.01)	***H04W 12/06***	(2011.01)
G06Q 20/04	(2012.01)	***H04W 12/08***	(2011.01)
G06Q 20/32	(2012.01)	***G06F 21/35***	(2013.01)
G07B 15/00	(2011.01)	***G06F 21/60***	(2013.01)
G07C 9/21	(2010.01)	***G06F 21/62***	(2013.01)
G06Q 30/06	(2013.01)	***G06Q 20/40***	(2012.01)
G06F 21/10	(2013.01)		
G06F 21/30	(2013.01)		
H04L 9/32	(2006.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.12.2020 PCT/SE2020/051153**

(87) Fecha y número de publicación internacional: **10.06.2021 WO21112746**

(96) Fecha de presentación y número de la solicitud europea: **01.12.2020 E 20895518 (7)**

(97) Fecha y número de publicación de la concesión europea: **17.04.2024 EP 4046093**

(54) Título: **Un permiso de acceso electrónico digital, personal y seguro**

(30) Prioridad:

06.12.2019 SE 1930393

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.10.2024

(73) Titular/es:

CODIQO AB (100.0%)
Rosendalsvägen 4A
13236 Saltsjö-boo, SE

(72) Inventor/es:

UNGERHOLM, MIKAEL

(74) Agente/Representante:

ANGOLOTI BENAVIDES, Joaquín

DESCRIPCIÓN

Un permiso de acceso electrónico digital, personal y seguro

La invención se refiere a un método para generar un permiso de acceso electrónico personal dirigido al mercado secundario no deseado y garantizar un proceso de entrada eficiente que valide tanto la identidad del cliente como el permiso del cliente para acceder al evento o lugar en un evento de escaneo

Antecedentes

El negocio de venta de entradas actual consiste en un mercado primario y un mercado secundario. En el mercado primario, las entradas originales se ofrecen a los compradores (fans) por un valor nominal que está definido por el promotor/artista y la empresa de entradas. A veces, las entradas se revenden en el mercado secundario, a menudo por un precio mucho más alto que el valor nominal.

Por un lado, el mercado secundario es beneficioso para el ecosistema del negocio de venta de entradas; el mercado presenta una oportunidad para revender una entrada en caso de que el propietario original de la entrada no pueda asistir al evento. Como resultado, puede haber un mayor número de asistentes al evento y aumentar las posibilidades de que el evento sea exitoso.

Por otro lado, el mercado secundario implica la venta de entradas con fines de lucro, lo que no es deseado por la mayoría de las partes interesadas en el ecosistema del negocio de la venta de entradas. Además del mercado secundario no deseado, existen entradas falsificadas, lo que empeora aún más la situación para los clientes que quieren comprar una entrada y confían en que la entrada les dará el derecho de acceder al evento durante el proceso de escaneo. Dado que no existe una solución segura que pueda separar una entrada auténtica de una falsa, prevalece el negocio de las entradas falsificadas.

Como el no deseado mercado secundario de "venta con fines de lucro" es lucrativo, hay muchos actores diferentes, tanto individuos como empresas, que intentan ganar dinero en el mercado secundario. Se usan bots para comprar entradas cuando se lanzan en el mercado primario y a continuación estas entradas pueden revenderse en el mercado secundario para obtener ganancias.

La forma en que los países regulan el mercado secundario difiere mucho. En Suecia, por ejemplo, las actividades del mercado secundario son legales.

Cualquiera, y también los bots, pueden usar varios correos electrónicos, varios ID de Apple y varios números de teléfono, etc., para iniciar sesión y comprar entradas en el mercado primario y revender las entradas para obtener ganancias en el mercado secundario. Algunos bots están optimizados para conseguir las mejores entradas y son muy rápidos, lo que dificulta que los compradores (fans) compitan con ellos. Los piratas informáticos, que usan bots, podrían usar tarjetas de crédito, correos electrónicos, contraseñas, etc., robados para hacerse con las entradas primarias. Por tanto, para crear una entrada personal es necesario verificar la identidad del cliente.

Algunos eventos requieren entradas personales por razones de seguridad, donde su nombre está escrito en la entrada (entrada personal) y la identificación (por ejemplo, carné de conducir y pasaporte) se verifica al entrar. Sin embargo, tener que mostrar la entrada y la identificación es un proceso lento y, por lo tanto, no se considera una solución eficaz. Si no se realiza ningún control de identificación, nadie sabrá quién está visitando el evento, lo que podría ser crucial, por ejemplo, en caso de incendio o ataque terrorista.

Saber quién tiene una entrada para un evento y quién asiste a un evento también resuelve un problema de marketing, ya que hoy en día sólo se sabe quién compró las entradas digitales (una persona puede comprar varias entradas para algunos amigos), no para quién eran las entradas y quién asiste realmente al evento, lo cual es una fortaleza desde el punto de vista del marketing

El proceso de escaneo actual, cuando se usan entradas personales, se puede describir con las siguientes etapas:

1. escaneo de un permiso de acceso (por ejemplo, una entrada) y
2. en una etapa separado mostrar una identificación física aprobada, tal como carné de conducir o pasaporte

lo cual requiere mucho tiempo y se considera un proceso ineficiente.

Existe una clara tendencia en el mercado de preferir las entradas móviles a las entradas en papel o en formato PDF (entradas electrónicas). En muchos casos, una entrada móvil se puede transferir fácilmente a otra persona a través de una billetera (por ejemplo, Apple Wallet) en un teléfono móvil, que puede usarse en el mercado secundario no deseado de "venta con fines de lucro". Es bastante fácil realizar una captura de pantalla de la entrada y pasar la entrada como imagen a otra persona. En algunas soluciones, el dispositivo móvil está vinculado con la entrada; sin embargo, el dispositivo móvil puede ser robado o prestado por otro usuario que puede usar la entrada con el teléfono prestado o robado. Al comprar una entrada a través de Internet, normalmente se usan la dirección de correo

electrónico, el nombre, los números de teléfono móvil, las contraseñas y las tarjetas de crédito como credenciales de autenticación para crear una cuenta e identificar al propietario de la entrada. Como una persona puede poseer direcciones de correo electrónico, números de teléfono móvil, dispositivos móviles y tarjetas de crédito de forma anónima, esta no es una buena solución para identificar a una persona en la entrada del evento o lugar, especialmente porque estos métodos de identificación también pueden ser robados. También se puede mantener el anonimato usando, por ejemplo, varias direcciones de correo electrónico y números de teléfono móvil. Con soluciones biométricas, tales como Touch ID y Face ID, varios usuarios pueden compartir y tener acceso a un mismo dispositivo, lo que dificulta saber quién de los usuarios registrados de Touch ID, o Face ID, está sosteniendo el dispositivo móvil en el evento de escaneo y por lo tanto dificulta identificar a la persona que entra en el evento. Si no se verifica, por ejemplo, con un servicio externo de identificación electrónica (como BankID en Suecia), que en realidad devuelve el nombre completo y el número personal del usuario al sistema, no hay posibilidad de validar la identidad real del usuario en un registro digital. ni en el proceso de escaneo de una entrada digital. Con la posibilidad de crear una cuenta con una identidad falsa y la posibilidad de que varias personas puedan acceder al dispositivo móvil vinculado con la entrada, todavía hay muchas oportunidades para habilitar un mercado secundario no deseado de "reventa con fines de lucro" y aún no hay posibilidad de validar si la persona que sostiene el dispositivo móvil es el verdadero propietario de la entrada y por lo tanto debe tener permiso para acceder al evento o tiene derecho a vender la entrada almacenada en el dispositivo móvil.

Hoy en día no existe ninguna solución digital segura que pueda, en la misma solución:

- Prevenir el mercado secundario no deseado de "reventa con fines de lucro" en una solución digital.
- abordar el mercado de falsificaciones
- habilitar el mercado secundario deseado (vender la entrada en caso de que el propietario original no pueda asistir) aún evitando que sea posible revender una entrada con fines de lucro fuera de la solución, y
- validar digitalmente la identidad del propietario de un entrada personal y digital y que el propietario tiene el permiso para acceder al evento y/o al lugar en un evento de escaneo y así ofrecer un proceso de entrada rápido y seguro y mejorar la eficiencia de las campañas de marketing y venta antes y después del evento.

Hay algunas soluciones en el mercado que abordan en parte los problemas descritos (por ejemplo, el fan verificado de Ticketmaster y las entradas verificadas, el código QR Motion del grupo Cellum, la solución de aplicación de DICE con un club cerrado para miembros y la solución biométrica de Blink Identity). La patente EP3442249 sugiere un método para que un servidor controle las entradas en una cartera de aplicación. El cliente usa una contraseña o datos de autenticación para identificarse y adquirir una entrada. A continuación, se vinculan la entrada y el dispositivo móvil. El propietario de una entrada puede entonces transferirla a un nuevo cliente autorizado conocido, lo que desgraciadamente hace posible transferir dinero del propietario al nuevo cliente autorizado fuera del sistema. Como la entrada está vinculada con el dispositivo móvil, significa que la entrada en sí no es personal y se necesita un pasaporte y un carné de conducir para entrar al evento o lugar donde se necesita la validación de la identidad. Además, no se describe un proceso de escaneo, por lo que es posible que un usuario no autorizado pueda tomar prestado el dispositivo móvil ya que la entrada está vinculada con un dispositivo móvil y no con una persona.

La publicación de patente estadounidense n.º 2016/0350547 A1 describe un sistema informático que usa datos de uso de entradas anteriores que indican una probabilidad de que una entidad respectiva use personalmente una entrada emitida para ella basándose en un historial de uso de entradas anteriores. Un controlador de entradas puede responder a las solicitudes de entradas determinando si se debe emitir una entrada a una entidad solicitante basándose en los datos de uso de entradas anteriores asociados con el perfil de la entidad solicitante y, de ser así, emitir una entrada a la entidad solicitante en formato electrónico. El sistema puede recibir una notificación de uso de entrada y actualizar los datos de uso de entrada anteriores asociados con el perfil de la entidad solicitante basándose en la notificación de uso de entrada, donde los datos de uso de entradas anteriores actualizados transmiten si la entidad solicitante presentó la entrada por sí misma.

La publicación de patente estadounidense n.º 2018/0173906 A1 describe un método de un sistema de identidad digital que genera un token compartido para autenticar a un portador ante un validador, en donde un almacén de datos del sistema de identidad digital contiene una pluralidad de atributos del portador. El sistema de identidad digital realiza las siguientes etapas: recibir en el sistema de identidad digital desde un portador una solicitud de token compartido electrónico, en donde la solicitud de token identifica al menos uno de los atributos del portador en el almacén de datos seleccionado para compartir con un validador; en respuesta a la solicitud de token electrónico, generar un token compartido, que es exclusivo de esa solicitud, para que el portador lo presente a un validador; asociar con el token compartido único en el sistema de identidad digital el al menos un atributo de portador identificado; y emitir al portador el token compartido único; y en donde la presentación posterior del token compartido único al sistema de identificación digital por parte de un validador hace que el al menos un atributo de portador asociado con el token compartido se ponga a disposición del validador mediante el sistema de identidad digital.

La técnica anterior no sugiere una solución digital única para todos los problemas descritos anteriormente, por lo que todavía prevalece el mercado secundario no deseado y que pocos eventos utilizan entradas personales, ya que el proceso de verificar la identidad manualmente con el carné de conducir o el pasaporte es demasiado engorroso.

Resumen de la invención

La invención está definida por las reivindicaciones adjuntas. La presente invención resuelve al menos uno de los problemas analizados anteriormente en cierta medida mediante el método mencionado inicialmente que genera un permiso de acceso electrónico personal (31), en un entorno que comprende un sistema (1) que incluye servidor(es), base(s) de datos y aplicación(es) y además el entorno comprende un dispositivo de comunicación móvil (2), un servicio de identificación electrónica (3) que es aceptado para identificación por las autoridades gubernamentales, un dispositivo de escaneo (4), Internet y/o redes de comunicación inalámbrica (6) y un cliente (5), abordando el mercado secundario no deseado y garantizando un proceso de entrada eficiente que valida tanto la identidad del cliente como el permiso del cliente para acceder a un evento o lugar en un evento de escaneo que comprende las etapas de

a descargar (etapa 1) de una aplicación al dispositivo de comunicación móvil (2)

b registrar (etapa 2), usando el dispositivo de comunicación móvil (2), el cliente (5) en el sistema (1), usando el servicio de identificación electrónica (3) en donde los datos de identidad del cliente (10) se envían al sistema (1) del servicio de identificación electrónica (3) y registrar así la identidad verificada del cliente

c almacenar (etapa 3) los datos de identidad del cliente (10) en el sistema (1) y emparejar (etapa 3) los datos de identidad del cliente (10) con un número de identificación único (11),

d almacenar (etapa 3) el número de identificación único (11) en el sistema (1)

e transmitir (etapa 4) desde el sistema (1) y almacenar el número de identificación único (11) en el dispositivo de comunicación móvil (2) después de lo cual el cliente (5) está

f comprando (etapa 5) un permiso de acceso electrónico (31) a un evento a través de una interacción entre el sistema (1) y el cliente (5), usando el dispositivo de comunicación móvil (2), a través de Internet y/o redes de comunicación inalámbrica (6), por lo que

g el sistema (1) está almacenando y emparejando (etapa 6) un número de cliente/evento único (12) con el número de identificación único (11) y

h transmitiendo el sistema (1) (etapa 8) el número de cliente/evento único (12) al dispositivo de comunicación móvil (2)

i generar (etapa 11) el permiso de acceso electrónico (31) en el dispositivo de comunicación móvil (2), autenticando primero la identidad del cliente (5) usando el servicio de identificación electrónica (3) (etapa 9), que está transmitiendo la identidad, los datos de identidad del cliente (10), al sistema (1), en donde la autorización es exitosa si la identidad del cliente (5), almacenada en el sistema (1), es la misma que la identidad transmitida desde el servicio de identificación electrónica (3) al sistema (1) y combinar, al menos, el número de identificación único (11), asociado y emparejado con los datos de identidad del cliente (10), y el número de cliente/evento único (12) usando un algoritmo (30) que genera el permiso de acceso electrónico (31) en el dispositivo de comunicación móvil (2), donde el permiso de acceso electrónico (31) es accesible durante un período de tiempo predefinido en el dispositivo de comunicación móvil (2), requerir al cliente (5) que genere un permiso de acceso electrónico válido (31), en el dispositivo de comunicación móvil (2), justo antes del proceso de escaneo en el evento y

j transmitir (etapa 12) el permiso de acceso electrónico generado (31) desde el dispositivo de telecomunicación móvil (2) al sistema (1)

k almacenar (etapa 13) el permiso de acceso electrónico generado (31) en el sistema (1)

l escanear (etapa 20) el permiso de acceso electrónico generado (31) en el dispositivo de comunicación móvil (2) con el dispositivo de escaneo (4) y transmitir (etapa 21) el permiso de acceso electrónico escaneado (31) al sistema (1)

m comparando el sistema (1) (etapa 22) el permiso de acceso electrónico escaneado (31) generado en el dispositivo de comunicación móvil (2) con el permiso de acceso electrónico almacenado (31) en el sistema y

n verificando el sistema (1) las transacciones con el permiso de acceso electrónico (31) registrado y por la presente

o validando el sistema (1) tanto los datos de identidad del cliente (10) como el permiso del cliente (5) para acceder al evento o lugar en un evento de escaneo y

p registrar (etapa 23) la transacción de escaneo en el permiso de acceso electrónico (31) en el sistema (1) y transmitir (etapa 24) el resultado de la validación al dispositivo de escaneo (4) desde el sistema (1) y mostrar (etapa 25) el resultado de la validación en el dispositivo de escaneo (4)

Preferentemente, la etapa i se logra creando una serie de, mínimo dos, números únicos separados en el tiempo que representan el permiso de acceso electrónico o creando un valor, que varía con el tiempo, que representa un permiso de acceso electrónico,

preferentemente, el período de tiempo predefinido en el que el permiso de acceso electrónico es accesible en el dispositivo de comunicación móvil puede estar en el intervalo de 1 s a 72 h, dependiendo del nivel de seguridad que el promotor elija establecer y el límite inferior puede ser uno cualquiera de 1 s , 10 s, 20 s, 30 s, 40 s, 50 s, 60 s, 2 min, 10 min, 30 min y el límite máximo puede ser uno cualquiera de 72 h, 24 h, 2 h, 30 min, 10 min, 1 min, 30 s, 10 s,

preferentemente, el permiso de acceso electrónico se genera, previa solicitud, justo antes del proceso de escaneo en el evento

preferentemente, que comprende retrovender un permiso de acceso electrónico al sistema a través de una interacción entre el sistema y el cliente, mediante la cual el permiso de acceso electrónico se marca como no válido en el sistema y se puede emitir un nuevo permiso de acceso electrónico único,

preferentemente, validar el derecho del cliente a retrovender el permiso de acceso electrónico confirmando la identidad del cliente usando un servicio de identificación electrónica que sea aceptado para identificación por las autoridades gubernamentales y verificar, en el sistema, que el cliente es el propietario legítimo del permiso de acceso electrónico verificando los datos almacenados para el cliente en el dispositivo de comunicación móvil y en el sistema,

preferentemente, la etapa i se logra usando un algoritmo que se almacena en el dispositivo de comunicación móvil,

preferentemente, cifrado de todos los datos transmitidos y almacenados, incluyendo números y algoritmos,

preferentemente, verificar la integridad de los datos, números y algoritmos almacenados, en el dispositivo de comunicación móvil y en el sistema, y si se pierde la integridad de los datos verificados, el permiso de acceso electrónico deja de ser válido,

preferentemente, previa solicitud, la invalidación de un permiso de acceso electrónico en el sistema,

preferentemente, la etapa o se logra validando, al menos, el nombre y la edad del cliente, y el derecho del cliente a entrar al evento o al lugar,

preferentemente, rastrear, autorizar y almacenar todas las transacciones en el permiso de acceso electrónico en el sistema,

preferentemente, que comprende controlar, por parte del sistema, cuántos permisos de acceso electrónico puede adquirir un cliente,

preferentemente, la etapa 1 se logra autenticando a los individuos que pueden usar el dispositivo de escaneo, la autenticación de un individuo se realiza a través de un servicio de identificación electrónica, y si el servicio de identificación electrónica está transmitiendo la misma identidad de un individuo que está almacenada en una lista de individuos autorizados en el sistema, al individuo que usa el servicio de identificación electrónica para autenticación se le concede acceso a la aplicación de escaneo,

preferentemente, validar la identidad del cliente comparando los datos recibidos desde el servicio de identificación electrónica con los datos almacenados en el sistema,

preferentemente, que comprende que una persona compra entradas para los amigos de la persona, registrados en el sistema, y que el sistema transmite los números de cliente/evento únicos a los amigos, después de que la persona ha pagado con éxito tanto la entrada de la persona como las entradas de los amigos de la persona, después de lo cual la persona y los amigos de la persona pueden generar sus permisos de acceso electrónico personales

Breve descripción de los dibujos

Figura A
La figura A muestra la comunicación entre el dispositivo de comunicación móvil y el sistema cuando el cliente se registra en el sistema, compra un acceso electrónico y genera un permiso de acceso electrónico de acuerdo con un ejemplo de la invención

Figura B
La figura B es un boceto esquemático sobre una generación del permiso de acceso electrónico de acuerdo con lo usado en la etapa 11 de la figura A. Se usan un número de identificación único (figura A, 11) y un número de cliente/evento único (figura A, 12) como entrada en el algoritmo

Figura C
La figura C muestra un proceso de escaneo de acuerdo con un ejemplo de la invención

Figura D
La figura D muestra un ejemplo de un entorno en el que se puede implementar la invención, que se compone de un sistema, un servicio de identificación electrónica, un dispositivo de comunicación móvil, un dispositivo de escaneo, Internet y/o redes de comunicación inalámbrica y un cliente

Descripción detallada de la solución

El entorno

Un sistema se compone de servidor(es), base(s) de datos y aplicación(es) (figura D, 1). El sistema está conectado a un servicio de identificación electrónica (figura D, 3) a través de Internet y redes de comunicación inalámbrica (figura D, 6). Por ejemplo, BankID es un servicio de identificación electrónica en sueco. La salida de un servicio de identificación electrónica al sistema se denomina datos de identidad del cliente. El sistema se comunica además con dispositivos de comunicación móviles (figura D, 2) y sus aplicaciones (que se descargan, por ejemplo, desde Apple Store) a través de redes de comunicación inalámbrica e Internet. Un cliente (figura D, 5) usa el dispositivo de comunicación móvil. En el proceso de escaneo, un dispositivo de escaneo (figura D, 4) puede comunicarse con el sistema así como con el dispositivo de comunicación móvil a través de un enlace visual (cámara o vídeo), a través de Internet o mediante un enlace/red de comunicación inalámbrica.

Conectar al individuo al permiso de acceso electrónico

Un permiso de acceso electrónico personal debe estar asociado a la identidad de un cliente. Una opción preferida para autorizar la identidad de un cliente es usar credenciales de autenticación junto con un servicio de identificación electrónica que sea aceptado para identificación por las autoridades gubernamentales (por ejemplo, BankID es un servicio de identificación electrónica en Suecia). Como solo puede haber un cliente por identificación electrónica, este es un método de autenticación mucho mejor que, por ejemplo, el correo electrónico con una contraseña o una tarjeta SIM o un dispositivo móvil, donde el propietario puede ser anónimo. Un cliente también puede tener varias direcciones de correo electrónico, ID de Apple, números de teléfono, tarjetas SIM, tarjetas de crédito, etc., lo que dificulta controlar cuántos permisos de acceso electrónico puede comprar un cliente. El uso de un servicio de identificación electrónica reducirá el riesgo de que bots, así como personas reales, compren más permisos de acceso electrónico de los que permiten las políticas, en comparación con, por ejemplo, el uso de direcciones de correo electrónico con contraseña como identificador de la identidad del cliente.

Después de descargar una aplicación al dispositivo de comunicación móvil (figura A, etapa 1) y cuando la identidad de un cliente ha sido validada por un servicio de identificación eléctrica, el cliente puede registrarse (figura A, etapa 2), utilizando los datos de identidad del cliente (figura A, 10) enviados al sistema desde el servicio de identificación eléctrica mediante el cual un número de identificación único (figura A, 11) se asocia y empareja con los datos de identidad del cliente (figura A, etapa 3). El número de identificación único (figura A, 11) se almacena a continuación en el sistema, después de lo cual el número de identificación único (figura A, 11) se transmite al dispositivo de comunicación móvil y se almacena en él (figura A, etapa 4). El número de identificación único (figura A, 11) se transmite a través de un enlace cifrado entre el sistema y el dispositivo de comunicación móvil.

Cuando el cliente ha comprado un permiso de acceso electrónico a través de una interacción con el sistema (figura A, etapa 5), se crea un número único por persona asociado con un evento, llamado número de cliente/evento único (figura A, 12), se almacena en el sistema y se empareja con el número de identificación único (figura A, etapa 6). Antes de que el número de cliente/evento único (figura A, 12), sea transmitido, el sistema verifica la integridad del número de identificación único (figura A, 11) en el móvil (figura A, etapa 7). A continuación, la validación se almacena en el sistema.

Si el número de identificación único (figura A, 11) en el dispositivo de comunicación móvil es el mismo que en el sistema, el número de cliente/evento único (figura A, 12) se transmite al dispositivo de comunicación móvil, donde se almacena (figura A, etapa 8). El número de cliente/evento único (figura A, 12) también se empareja con la identificación de cliente única (figura A, 11) en el dispositivo de comunicación móvil.

Una persona puede comprar entradas para los amigos de la persona, si estos están registrados en el sistema, y el sistema está transmitiendo los números de cliente/evento únicos a los amigos, después de que la persona haya pagado exitosamente tanto la entrada de la persona como la entrada de los amigos de la persona. A continuación, la persona y los amigos de la persona pueden generar sus permisos de acceso electrónico personales.

Los consentimientos del cliente se otorgan antes de almacenar cualquier dato personal de acuerdo con las

regulaciones y leyes aplicables.

Generación del permiso de acceso electrónico digital, personal y seguro

La aplicación descargada incluye un algoritmo que puede generar un permiso de acceso electrónico. Con el número de identificación único (figura A, 11) y el número de cliente/evento único (figura A, 12) como entrada al algoritmo (figura B, 30), este puede generar una serie de, mínimo dos, números únicos que representen el permiso de acceso electrónico (figura B, 31). Otra opción para generar un permiso de acceso electrónico es que el algoritmo en el dispositivo de comunicación móvil esté generando un valor que varía, por ejemplo, con el tiempo, de modo que el valor del permiso de acceso electrónico diferirá con el tiempo.

Para indicarle al algoritmo que inicie la generación del permiso de acceso electrónico, en cualquier momento, la solución preferida es que el cliente necesite, exitosamente, autenticar su identidad con un servicio de identificación electrónica (figura A, etapa 9). La autenticación es exitosa si la identidad del cliente, almacenada en el sistema, es la misma que la identidad transmitida desde el servicio de identificación electrónica al sistema. Si la autenticación no es exitosa, el permiso de acceso electrónico se marca como no válido en el sistema, lo que será reconocido en el proceso de escaneo más adelante. Antes de la generación del permiso de acceso electrónico, se verifica la integridad de los datos en el dispositivo de comunicación móvil y en el sistema (figura A, etapa 10).

A continuación, el permiso de acceso electrónico se genera en el dispositivo de comunicación móvil (figura A, etapa 11) y se transmite (figura A, etapa 12), a través de un enlace cifrado, al sistema donde se almacena (figura A, etapa 13). El algoritmo está diseñado para que cada cliente haya comprado un permiso de acceso electrónico único.

El permiso de acceso electrónico se puede almacenar en el dispositivo de comunicación móvil hasta que se solicite su eliminación, pero la solución preferida, por razones de seguridad, es que el permiso de acceso electrónico se elimine automáticamente en el dispositivo de comunicación móvil después de un período de tiempo definido. Esto requiere que el cliente genere un permiso de acceso electrónico válido justo antes del proceso de escaneo en el evento. El permiso de acceso electrónico, en el dispositivo de comunicación móvil, se puede eliminar automáticamente después de un período de tiempo definido, que puede estar en el intervalo de 1 s a 72 h, dependiendo del nivel de seguridad que el promotor elija establecer. El límite inferior puede ser uno cualquiera de 1 s, 10 s, 20 s, 30 s, 40 s, 50 s, 60 s, 2 min, 10 min, 30 min. El límite máximo puede ser uno cualquiera de 72 h, 24 h, 2 h, 30 min, 10 min, 1 min, 30 s, 10 s. El permiso de acceso electrónico se puede generar previa solicitud, asegurándose de que el titular del dispositivo móvil sea el propietario legítimo del permiso de acceso electrónico. Obviamente, se puede generar un permiso de acceso electrónico válido, incluso si un permiso de acceso electrónico previamente se ha eliminado en el dispositivo de comunicación móvil después de un período de tiempo definido, con un número de identificación único válido (figura A, 11) y un número de cliente/evento único válido (figura A, 12), almacenado en el dispositivo de comunicación móvil, como entrada al algoritmo (figura B, 30) y mostrarse dentro del período de tiempo definido como se ha descrito anteriormente. La validación y comparación del permiso de acceso electrónico escaneado y el permiso de acceso electrónico almacenado en el sistema se realiza en el proceso de escaneo.

Escaneo seguro y un proceso de entrada sin errores

Se descarga una aplicación de escaneo en un dispositivo de escaneo (figura D, 4). Si el permiso de acceso electrónico estuviera representado por un número único estático y, por ejemplo, por un código QR, se podría enviar una imagen a una persona no autorizada, que podría utilizar la imagen copiada del permiso de acceso electrónico para obtener acceso al evento/lugar.

Para evitar este escenario, la presente invención sugiere un permiso de acceso electrónico representado por una serie de, mínimo dos, números únicos que se transmiten en un orden determinado y en intervalos de tiempo predefinidos desde el dispositivo de comunicación móvil al dispositivo de escaneo (figura C, etapa 20). Como el dispositivo de escaneo sabe cuántos números únicos que están representando el permiso de acceso electrónico y el tiempo entre cada número único transmitido, el dispositivo de escaneo puede recopilar todos los números que representan el permiso de acceso electrónico en el proceso de escaneo. Una vez que el dispositivo de escaneo haya recibido el permiso de acceso electrónico, lo transmitirá al sistema (figura C, etapa 21). A continuación, el sistema compara el permiso de acceso electrónico del dispositivo de comunicación móvil con el permiso de acceso electrónico del sistema (figura C, etapa 22). Si son iguales, al cliente tiene se le otorga acceso al evento/lugar. El sistema también verifica si el permiso de acceso electrónico está marcado como no válido en el sistema y, de ser así, al cliente no se le otorga acceso al evento/lugar. Obviamente, el permiso de acceso electrónico almacenado en el sistema está vinculado al cliente a través del número de identificación único almacenado en el sistema (figura A, 11) y el número de cliente/evento único (figura A, 12). La transacción escaneada queda registrada en el sistema (figura C, etapa 23). Se transmite un mensaje al dispositivo de escaneo con el resultado de la validación del permiso de acceso electrónico (figura C, etapa 24). El resultado de la validación se muestra en el dispositivo de escaneo (figura C, etapa 25) y el evento de escaneo se almacena en el sistema.

Como se mencionó anteriormente, una alternativa para dificultar la copia de un permiso de acceso electrónico podría ser que el algoritmo en el dispositivo de comunicación móvil genere un valor que varíe, por ejemplo, con el tiempo, de modo que el valor del permiso de acceso electrónico diferirá con el tiempo. En esta alternativa, el sistema y el

dispositivo de comunicación móvil necesitarán generar permisos de acceso electrónico coincidentes en el sistema y en el dispositivo de comunicación móvil en todo momento. El método del proceso de escaneo es el mismo que en la figura C para esta alternativa.

Como el permiso de acceso electrónico se puede generar en el dispositivo de comunicación móvil previa solicitud, el proceso de escaneo remedia tanto la identidad del cliente como el derecho del cliente a acceder al evento/lugar en un solo evento de escaneo y, por lo tanto, ahorra mucho tiempo al entrar en un evento/lugar.

Si el cliente no trae el dispositivo de comunicación móvil al evento, una opción es escanear la identificación física del cliente, tal como por ejemplo el carné de conducir o el pasaporte, con un dispositivo de escaneo y comparar los datos de identidad del cliente almacenados en el sistema con los datos de identidad del cliente almacenados en la identificación física. Si coinciden, se concede al cliente el acceso al evento/lugar, previa verificación de si el permiso de acceso electrónico es válido en el sistema.

Las personas autorizadas para usar el dispositivo de escaneo aparecen en el sistema antes de su uso. La autenticación de una persona física se realiza a través de un servicio de identificación electrónica. Si el servicio de identificación electrónica transmite la misma identidad que está almacenada en la lista del sistema, el individuo que usa el servicio de identificación electrónica para la autenticación tiene acceso a la aplicación de escaneo.

Prevenir el mercado secundario no deseado sin transferencias de dinero fuera del sistema

El mercado secundario no deseado es posible si una persona puede vender un permiso de acceso a otra persona conocida y el permiso de acceso comprado puede entregarse a la persona que compró el permiso de acceso. Como el vendedor y el comprador se conocen, el comprador puede compensar al vendedor por entregar el permiso de acceso además del valor nominal.

La presente invención sugiere que el vendedor nunca conocerá la identidad del comprador. En caso de que el propietario no pueda asistir al evento para el cual ha comprado un permiso de acceso electrónico, es posible retrovender el permiso de acceso electrónico al sistema a través de una interacción entre el cliente y el sistema. El permiso de acceso electrónico se marca entonces como no válido en el sistema, lo que también se notifica al cliente (por ejemplo, mediante un mensaje push). Por la presente, el sistema puede vender un nuevo permiso de acceso electrónico a un cliente registrado sin la participación del cliente que retrovendió su permiso de acceso electrónico al sistema.

El permiso de acceso electrónico no se puede entregar directamente de una persona a otra ya que el permiso de acceso electrónico es personal y está integrado con la identidad de un cliente.

Seguridad

Todos los números y enlaces usados en los procesos anteriores están preferentemente cifrados. Para garantizar la integridad de los datos antes de que se usen en un proceso, se verifica la integridad de los datos. La opción preferible es utilizar una solución de cadena de bloques (*blockchain*) para realizar verificaciones de integridad en el sistema y en el dispositivo de comunicación móvil, ya que los datos almacenados en una cadena de bloques son inmutables. Con una solución de cadena de bloques, la integridad de los datos no almacenados en la cadena de bloques se puede verificar con tecnología hash. Como se verifica la integridad de los datos, estos no se pueden manipular sin ser descubierto. Si los datos han sido manipulados el permiso de acceso electrónico se marca como no válido.

Falsificaciones

Como el permiso de acceso electrónico sugerido por la invención es personal, es difícil crear una falsificación o copia creíble sin robar la identificación electrónica de una persona. No se puede generar un permiso de acceso electrónico válido sin una autenticación exitosa de la identidad del cliente. Además, no se puede suministrar un permiso de acceso electrónico válido desde un dispositivo de comunicación móvil a otro dispositivo de comunicación móvil. De este modo, es fácil reconocer un permiso de acceso electrónico válido y diferenciarlo de una falsificación.

Transacciones con permiso de acceso electrónico

A medida que el sistema y el dispositivo de comunicación móvil están conectados, todas las transacciones en el permiso de acceso electrónico se pueden rastrear, autorizar y almacenar en la solución. En el sistema se puede definir qué transacciones están permitidas y cuándo están permitidas. Ejemplos de transacciones con un permiso de acceso electrónico pueden ser, pero sin limitación, marcar un permiso de acceso electrónico como "no válido", marcar un permiso de acceso electrónico como "escaneado", registrar cuándo un cliente específico está transmitiendo el permiso de acceso electrónico al sistema o marcar que un permiso de acceso electrónico se ha vendido.

Breve descripción de los dibujos

Figura A
La figura A muestra la comunicación entre el dispositivo de comunicación móvil y el sistema cuando el cliente se registra en el sistema, compra un acceso electrónico y genera un permiso de acceso electrónico de acuerdo con un ejemplo de la invención

Figura B
La figura B es un boceto esquemático sobre una generación del permiso de acceso electrónico de acuerdo con lo usado en la etapa 11 de la figura A. Se usan un número de identificación único (figura A, 11) y un número de cliente/evento único (figura A, 12) como entrada en el algoritmo

Figura C
La figura C muestra un proceso de escaneo de acuerdo con un ejemplo de la invención

Figura D
La figura D muestra un ejemplo de un entorno en el que se puede implementar la invención, que se compone de un sistema, un servicio de identificación electrónica, un dispositivo de comunicación móvil, un dispositivo de escaneo, Internet y/o redes de comunicación inalámbrica y un cliente

REIVINDICACIONES

1. Un método para generar un permiso de acceso electrónico personal (31), en un entorno que comprende un sistema (1) que incluye servidor(es), base(s) de datos y aplicación(es) y además el entorno comprende un dispositivo de comunicación móvil (2), un servicio de identificación electrónica (3), un dispositivo de escaneo (4), Internet y/o redes de comunicación inalámbrica (6) y un cliente (5),

registrar, usando el dispositivo de comunicación móvil (2), el cliente (5) en el sistema (1), usando el servicio de identificación electrónica (3), en donde el servicio de identificación electrónica (3) es aceptado para identificación por las autoridades gubernamentales y en donde los datos de identidad del cliente (10) se envían al sistema (1) desde el servicio de identificación electrónica (3) y, de este modo, se registra la identidad verificada del cliente almacenando los datos de identidad del cliente (10) en el sistema (1) y emparejando los datos de identidad del cliente. (10) con un número de identificación único (11),
comprar, usando el dispositivo de comunicación móvil (2), un permiso de acceso electrónico (3) al evento o lugar, en donde la compra comprende:

asociar un número de cliente/evento único (12) con el número de identificación único (11);
almacenar el número de cliente/evento asociado (12) y el número de identificación único (11) en el sistema (1); y
transmitir el número de cliente/evento (12) al dispositivo de comunicación móvil (2);

generar el permiso de acceso electrónico (31) en el dispositivo de comunicación móvil (2), en donde la generación comprende:

autenticar la identidad del cliente usando el servicio de identificación electrónica (3) para garantizar que los datos de identidad del cliente (10) generados por el servicio de identificación electrónica (3) sean idénticos a los datos de identidad del cliente (10) almacenados en el sistema (1), en donde
la autenticación es exitosa si hay una coincidencia entre los datos de identidad del cliente (10);
y
combinar el número de identificación único (11) y el número de cliente/evento (12) usando un algoritmo (30) en el dispositivo de comunicación móvil (2) para generar el permiso de acceso electrónico (31), en donde el permiso de acceso electrónico (31) tiene una validez limitada en el tiempo en el dispositivo de comunicación móvil (2), requiriendo que el cliente genere el permiso de acceso electrónico (31) dentro de un período de tiempo particular antes de un evento de escaneo en una entrada del evento o lugar;

transmitir el permiso de acceso electrónico generado (31) desde el dispositivo de comunicación móvil (2) al sistema (1)
almacenar el permiso de acceso electrónico generado (31) en el sistema (1)
escanear el permiso de acceso electrónico generado (31) en el dispositivo de comunicación móvil (2) con el dispositivo de escaneo (4) y transmitir el permiso de acceso electrónico escaneado (31) al sistema (1)
comparando el sistema (1) el permiso de acceso electrónico escaneado (31) generado en el dispositivo de comunicación móvil (2) con el permiso de acceso electrónico almacenado (31) en el sistema
y
verificando el sistema (1) las transacciones en el permiso de acceso electrónico (31) registrado
validando el sistema (1) tanto los datos de identidad del cliente (10) como el permiso del cliente (5) para acceder al evento o lugar en un evento de escaneo, evitando el mercado secundario y garantizando un proceso de entrada eficiente y
registrar la transacción de escaneo en el permiso de acceso electrónico (31) en el sistema (1) y transmitir el resultado de la validación al dispositivo de escaneo (4) desde el sistema (1) y mostrar el resultado de la validación en el dispositivo de escaneo (4).

2. El método de la reivindicación 1, en donde generar el permiso de acceso electrónico se logra creando una serie de, mínimo dos, números únicos separados en el tiempo que representan el permiso de acceso electrónico (31) o creando un valor, que varía con el tiempo, que representa el permiso de acceso electrónico (31).

3. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además que el período de tiempo predefinido puede estar en el intervalo de 1 a 72 h, dependiendo del nivel de seguridad que el promotor elija establecer y el límite inferior puede ser uno cualquiera de 1 s, 10 s, 20 s, 30 s, 40 s, 50 s, 60 s, 2 min, 10 min, 30 min y el límite máximo puede ser uno cualquiera de 72 h, 24 h, 2 h, 30 min, 10 min, 1 min, 30 s, 10 s.

4. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además que el permiso de acceso electrónico (31) se genera, previa solicitud, justo antes del proceso de escaneo en el evento.

5. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además retrovender el permiso de acceso electrónico (31) al sistema (1) a través de una interacción entre el sistema (1) y el cliente (5), mediante la cual el permiso de acceso electrónico (31) se marca como no válido en el sistema (1) y se puede emitir un nuevo permiso de acceso electrónico único (31).

6. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además validar el derecho del cliente (5) a retrovender el permiso de acceso electrónico (31) confirmando la identidad del cliente (5) usando el servicio de identificación electrónica (3) que es aceptado para la identificación por parte de autoridades gubernamentales y verificar, en el sistema, que el cliente (5) es el propietario legítimo del permiso de acceso electrónico (31) verificando los datos almacenados para el cliente (5) en el dispositivo de comunicación móvil (2) y en el sistema (1).

7. El método de la reivindicación 1, en donde generar el permiso de acceso electrónico (31) se logra usando el algoritmo (30) que está almacenado en el dispositivo de comunicación móvil (2).

8. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además el cifrado de todos los datos transmitidos y almacenados, incluyendo números y algoritmos.

9. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además verificar la integridad de los datos, números y algoritmos almacenados en el dispositivo de comunicación móvil (2) y en el sistema (1), y si se pierde la integridad de los datos verificados, el permiso de acceso electrónico (31) deja de ser válido.

10. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende, además, previa solicitud, invalidar el permiso de acceso electrónico (31) en el sistema (1).

11. El método de la reivindicación 1, en donde validar tanto los datos de identidad del cliente (10) como el permiso del cliente (5) para acceder al evento o lugar se logra validando, al menos, el nombre y la edad del cliente (5), y el derecho del cliente (5) a entrar al evento o al lugar.

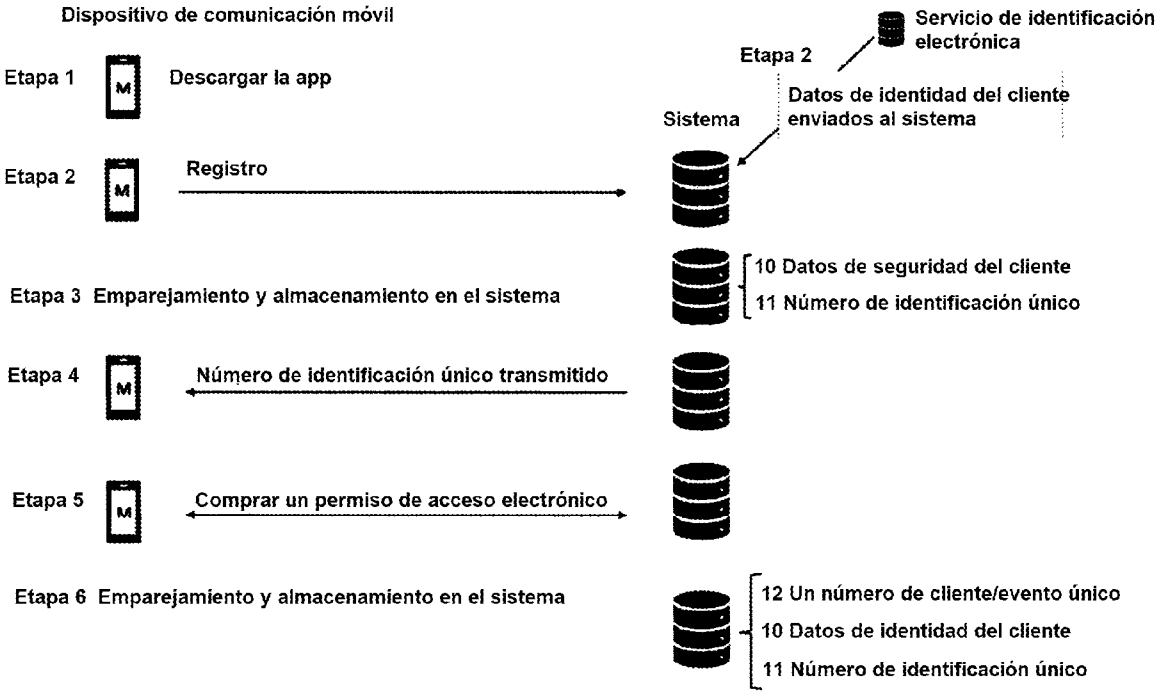
12. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además rastrear, autorizar y almacenar todas las transacciones en el permiso de acceso electrónico (31) en el sistema (1).

13. El método de la reivindicación 1, en donde validar tanto los datos de identidad del cliente (10) como el permiso del cliente (5) para acceder al evento o lugar en un evento de escaneo se logra autenticando a los individuos que pueden usar el dispositivo de escaneo (4), la autenticación de un individuo se realiza a través del servicio de identificación electrónica (3), y si el servicio de identificación electrónica (3) está transmitiendo la misma identidad del individuo que está almacenada en una lista de individuos autorizados en el sistema (1), al individuo que usa el servicio de identificación electrónica (3) para autenticación se le concede acceso a la aplicación de escaneo.

14. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además validar la identidad del cliente (5) comparando los datos recibidos desde el servicio de identificación electrónica (3) con los datos almacenados en el sistema (1).

15. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además que una persona compra entradas para los amigos de la persona, registrados en el sistema (1), y que el sistema (1) transmite los números de cliente/evento únicos a los amigos, después de que la persona ha pagado con éxito tanto la entrada de la persona como las entradas de los amigos de la persona, después de lo cual la persona y los amigos de la persona pueden generar sus permisos de acceso electrónico personales.

Figura A


Dispositivo de comunicación móvil
Servicio de identificación electrónica
Etapa 1
Descargar la app
Etapa 2
Datos de identidad del cliente enviados al sistema
Sistema
Etapa 2
Registro
10 Datos de seguridad del cliente
11 Número de identificación único
Etapa 3 Emparejamiento y almacenamiento en el sistema
Etapa 4
Número de identificación único transmitido
Etapa 5
Comprar un permiso de acceso electrónico
12 Un número de cliente/evento único
10 Datos de identidad del cliente
11 Número de identificación único
Etapa 6 Emparejamiento y almacenamiento en el sistema

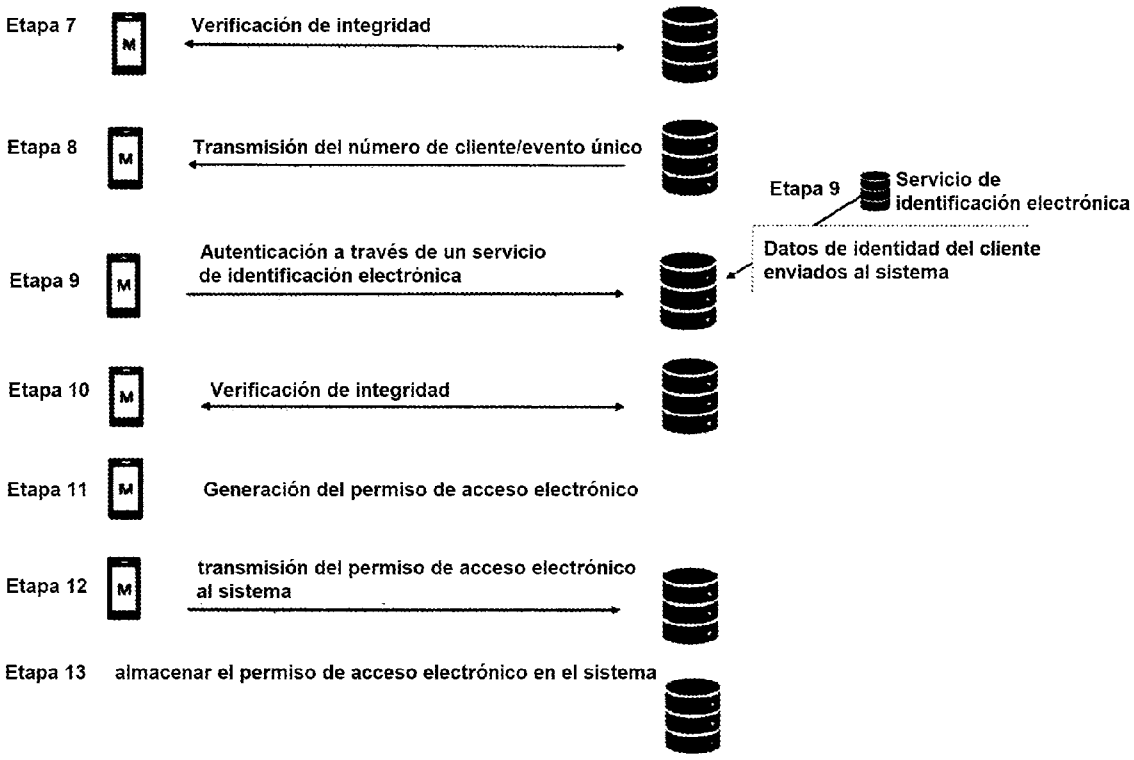

Etapa 7
Verificación de integridad
Etapa 8
Transmisión del número de cliente/evento único
Etapa 9
Servicio de identificación electrónica
Etapa 9
Autenticación a través de un servicio de identificación electrónica
Datos de identidad del cliente enviados al sistema
Etapa 10
Verificación de integridad
Etapa 11
Generación del permiso de acceso electrónico
Etapa 12
transmisión del permiso de acceso electrónico al sistema
Etapa 13
almacenar el permiso de acceso electrónico en el sistema

Figura B

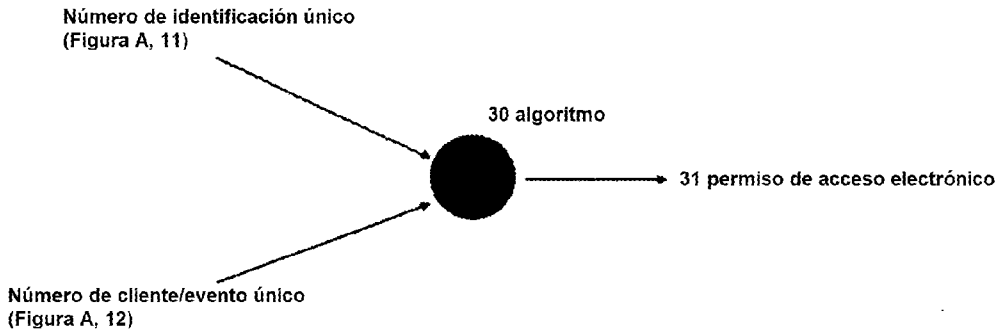

Número de identificación único
(Figura A, 11)
30 algoritmo
31 permiso de acceso electrónico
Número de cliente/evento único
(Figura A, 12)

Figura C

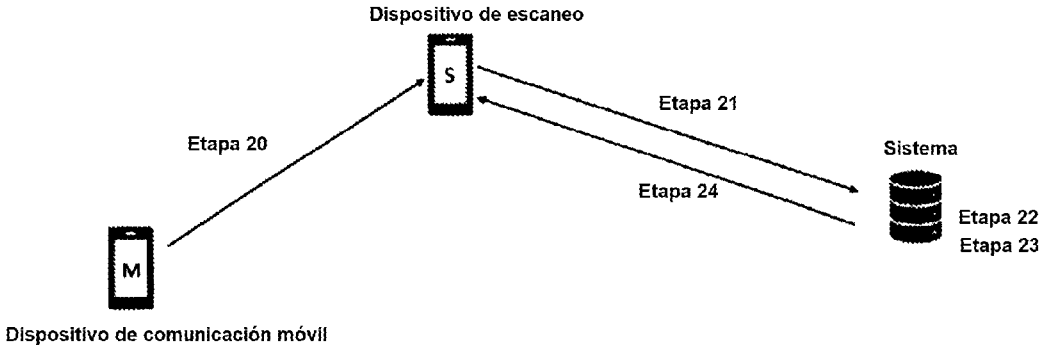


Figura D