(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 906 890**

(51) Int. CI.:

G07C 9/00 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.05.2018 E 18173626 (5)**

(97) Fecha y número de publicación de la concesión europea: **29.12.2021 EP 3567555**

(54) Título: **Procedimiento para manejar un sistema de acceso**

(30) Prioridad:

09.05.2018 EP 18171576

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.04.2022

(73) Titular/es:

EMZ-HANAUER GMBH & CO. KGAA (100.0%)
Siemensstrasse 1
92507 Nabburg, DE

(72) Inventor/es:

PINDL, STEFAN;
ALTENHOFER, HERBERT y
PLÖSSL, KLAUS

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento para manejar un sistema de acceso

La invención se refiere a un procedimiento para manejar un sistema de acceso para un dispositivo de acceso, en particular para un contenedor de basura.

Con frecuencia se proporcionan contenedores de basura de gran capacidad, que son utilizados por varios hogares, para la eliminación de la basura doméstica. Los contenedores de basura de este tipo pueden, por ejemplo, pertenecer a una comunidad de vecinos o a un municipio. Los contenedores de basura de este tipo comprenden por regla general un dispositivo de acceso de modo que los usuarios autorizados obtengan un acceso a tales contenedores de basura. La autorización también se puede volver a bloquear, por ejemplo, si no se pagan los costes de eliminación de basuras. Un acceso de este tipo se puede realizar por medio de los más diversos sistemas electrónicos. Por el estado de la técnica se conoce, por ejemplo, asignar un código de identificación a un usuario. Este código de identificación se introduce, por ejemplo, a través de un teclado numérico reducido dispuesto en el contenedor de basura. Sin embargo, los sistemas de este tipo son poco prácticos para el usuario, dado que ha de tener siempre a mano los datos de acceso. Asimismo, la pérdida de los datos de acceso conlleva un proceso de administración complejo.

El uso anterior de campos de entrada de PIN o etiquetas y tarjetas RFID tiene además la desventaja de que se requiere hardware adicional y/o conocimientos adicionales por parte del usuario. Los costes y gastos de administración adicionales son necesarios, dado que el hardware debe entregarse o enviarse al usuario. Asimismo, la protección contra el uso indebido es difícil dependiendo del procedimiento específico. Un límite de tiempo para el acceso es difícil o imposible de implementar; con el acceso basado en llaves, por ejemplo, habría que reemplazar todas las cerraduras y redistribuir todas las llaves.

El documento US 2015/307273 A1 divulga un procedimiento de acuerdo con el preámbulo de la reivindicación 1.

Es objetivo de la presente invención proporcionar un procedimiento mejorado para manejar un sistema de acceso para un dispositivo de acceso.

Este objetivo se consigue mediante un procedimiento de acuerdo con la reivindicación 1.

El acceso a un contenedor de basura con acceso restringido por un dispositivo de acceso se concede así al usuario de la forma más cómoda posible, dado que únicamente necesita tener a mano un aparato de comunicación. La solución funciona sin hardware adicional y sin conocimiento adicional por parte del cliente. En el momento del acceso, no es absolutamente necesaria una conexión activa al sistema central (para la transferencia de datos y autenticación). La protección contra el uso indebido está garantizada, ya que se elimina la capacidad de copiar tarjetas disponibles en el mercado (y, por lo tanto, el uso indebido). Asimismo, el acceso se puede restringir regionalmente así como en términos de tiempo. La solución es fácilmente escalable y fácilmente configurable para usuarios cambiantes.

Los datos de autenticación autorizan preferentemente el acceso a varios dispositivos de acceso, en particular contenedores de basura.

Por un intervalo de validez predeterminado se entiende preferentemente un intervalo de validez en el tiempo. Por ejemplo, esto significa el periodo de contrato de un usuario con una empresa de eliminación de basuras correspondiente.

Por una zona de validez predeterminada también se puede entender acumulativa o alternativamente un intervalo de validez espacial. En consecuencia, el acceso de un usuario podría estar restringido a varios dispositivos de acceso, preferentemente contenedores de basura, en un área espacial específica, tal como por ejemplo una comunidad de vecinos, un municipio o similar.

Por un canal de comunicación se entenderá una trayectoria de transmisión. Una trayectoria de transmisión de este tipo conecta un emisor y un receptor. Este emisor o receptor es ventajosamente parte de una interfaz de comunicación. Por consiguiente, el aparato de comunicación presenta una primera interfaz de comunicación. La primera interfaz de comunicación está conectada con una tercera interfaz de comunicación del sistema de gestión de datos a través de un primer canal de comunicación, en donde por la conexión ha de entenderse la posibilidad de un intercambio de datos. El aparato de comunicación presenta asimismo una segunda interfaz de comunicación, que está conectada con la cuarta interfaz de comunicación del dispositivo de acceso por medio del segundo canal de comunicación, mediante lo cual al menos los datos de autenticación se transmiten al dispositivo de acceso por medio de una tecnología inalámbrica.

Por un acceso al dispositivo de acceso puede entenderse, por ejemplo, un desbloqueo de una compuerta de basura o el desenganche de una cerradura que cierra el contenedor de basura.

Según una forma de realización especialmente preferida, el aparato de comunicación es un aparato de procesamiento de datos portátil, por ejemplo, un teléfono móvil, un teléfono inteligente, una tableta o un ordenador portátil. Naturalmente, la presente invención no se limita a esta enumeración y también se pueden considerar otros aparatos de procesamiento de datos similares para la aplicación. El uso de teléfonos móviles o teléfonos inteligentes está tan extendido que la gran mayoría de los miembros de una comunidad de vecinos o municipio correspondiente tiene un teléfono inteligente de este tipo. El usuario, por consiguiente, no necesita ningún otro dispositivo para registrarse o autenticarse, ni tiene que recordar los datos de acceso correspondientes.

Preferentemente, el aparato de comunicación presenta un equipo de control en el que está instalado un software, también denominado aplicación, por medio del cual se permite el registro del usuario registrarse en el sistema de gestión de datos y/o por medio del cual se puede controlar el intercambio de datos a través de un segundo canal de comunicación entre el aparato de comunicación y el dispositivo de acceso, o entre la primera interfaz de comunicación del aparato de comunicación y la tercera interfaz de comunicación del sistema de gestión de datos. Ventajosamente, el aparato de comunicación comprende un equipo de visualización.

Según otra forma de realización preferida, el primer canal de comunicación es una conexión móvil. Preferentemente, la conexión es una conexión GSM o una conexión UMTS o una conexión GPRS o una conexión LTE. Naturalmente, también se tienen en cuenta otras conexiones, tales como conexiones de radio, por ejemplo, en la banda ISM o WLAN.

Según una forma de realización especialmente preferida, la conexión inalámbrica del segundo canal de comunicación, o la tecnología inalámbrica, es una conexión/tecnología NFC (Near Field Communication (comunicación de campo cercano)) o una conexión/tecnología RFID (radio-frequency identification (identificación por radiofrecuencia)). Sin embargo, también sería concebible usar otras tecnologías inalámbricas tales como Bluetooth o LAN inalámbrica. Por lo tanto, la segunda interfaz de comunicación del aparato de comunicación y la cuarta interfaz de comunicación del sistema de gestión de archivos están equipadas con la tecnología inalámbrica correspondiente.

La tecnología NFC como también la tecnología RFID usan campos magnéticos alternos de alta frecuencia para la transmisión de datos. La tecnología RFID es por regla general una denominada transmisión "sin conexión". En este sentido se usa un transpondedor pasivo, que recibe energía del campo alterno de un dispositivo de lectura. La tecnología NFC proporciona además lo que se conoce como transmisión "basada en conexión". En el caso de transmisión basada en conexión o también transmisión entre pares, se establece una transmisión entre dos transmisores equivalentes.

Entretanto, una pluralidad de teléfonos inteligentes disponibles comercialmente ahora están equipados con un equipo NFC. Únicamente dos participantes pueden estar involucrados en una transmisión de datos, el denominado iniciador, que actúa como transmisor de información y un receptor, que recibe esta información.

La tecnología NFC también proporciona una transmisión "sin conexión" análoga a la tecnología RFID. Una transmisión de este tipo a menudo se denomina transmisión pasiva. En este caso únicamente el iniciador genera el campo magnético de alta frecuencia. El receptor puede transmitir datos por medio de una modulación de carga. A este respecto, tiene lugar una absorción de energía del campo magnético por un circuito resonante sintonizado especialmente en el receptor, después de lo cual reacciona el iniciador.

En la transmisión "basada en conexión" o también activa, tanto el iniciador como el receptor generan un campo magnético de alta frecuencia. En primer lugar, se lleva a cabo el llamado "apretón de manos", en el que tiene lugar una autenticación y en el que se seleccionan distintos ajustes, tales como, por ejemplo, la velocidad de transmisión óptima. A continuación, se lleva a cabo el intercambio de datos. Debido a la autenticación, esta transmisión activa se considera mucho más segura en comparación con la transmisión pasiva.

Según una forma de realización preferida, el dispositivo de acceso se activa antes de iniciar el intercambio de datos. Esto puede tener lugar, por ejemplo, a través de un botón o un elemento similar. Como alternativa, la activación se puede llevar a cabo mediante una "Low Power Card Detection" (detección de tarjeta de baja potencia) (LPCD), que detecta automáticamente la presencia de un aparato de comunicación habilitado para NFC en la proximidad directa.

Según otra forma de realización preferida, la segunda interfaz de comunicación del aparato de comunicación tiene que activarse, es decir, la función NFC se activa.

Preferentemente el software/la aplicación permanece activo/a en segundo plano de modo que la función NFC permanece activada. Después de un registro exitoso, el usuario puede por lo tanto obtener acceso al dispositivo de acceso en cualquier momento por medio del aparato de comunicación.

Según una forma de realización preferida, el dispositivo de acceso presenta un segundo equipo de control que controla correspondientemente un equipo de desbloqueo si el usuario está autorizado. En la configuración preferida como contenedor de basura, se desbloquea por lo tanto una esclusa de basura. El usuario puede así arrojar su

basura al contenedor. En el momento del intercambio de datos a través del segundo canal de comunicación, no tiene que haber conexión alguna del aparato de comunicación con el sistema de gestión de datos por medio de un primer canal de comunicación para desbloquear el dispositivo de acceso.

Según otra forma de realización preferida, en la etapa a) datos de identificación de usuario, datos de identificación de aparato del aparato de comunicación y un código de registro, que se proporciona por un operador, se transmiten al sistema de gestión de datos mediante el aparato de comunicación.

Preferentemente, los datos de autenticación comprenden preferentemente datos clave, información de validez así como un código de región. El equipo de control del dispositivo de acceso puede utilizar estos datos para comprobar si se concede el acceso. Si la hora actual está disponible en el equipo de control del dispositivo de acceso, estos datos también se pueden usar para verificar la validez temporal independientemente del equipo de control del aparato de comunicación.

El operador es en este sentido una empresa de eliminación de basuras, un municipio o similar. El sistema de gestión de archivos importa en primer lugar los datos de usuario del operador. Estos datos de usuario comprenden el nombre y la dirección del usuario, datos de identificación de usuario, tales como, por ejemplo, el número de contrato, un código de región y dos códigos de registro. Los códigos de registro se envían al usuario, por ejemplo, por carta, correo electrónico o similar.

El intervalo de validez espacial se define preferentemente por medio del código de región.

Preferentemente, a un usuario se le puede proporcionar un número predeterminado de datos de autenticación. Por consiguiente, el usuario puede equipar varios aparatos de comunicación con datos de autenticación correspondientes, de modo que obtenga un acceso al dispositivo de acceso por medio de varios aparatos de comunicación.

Según una forma de realización preferida, los datos de identificación de usuario y el código de registro pueden introducirse por lectura por medio de un escáner QR del aparato de comunicación. Por lo tanto se permite un registro especialmente rápido.

Preferentemente, durante el uso del aparato de comunicación (5) en el dispositivo de acceso, el aparato de comunicación no tiene conexión alguna con el sistema de gestión de archivos a través del primer canal de comunicación. Esto garantiza que el dispositivo de acceso pueda abrirse incluso si la cobertura de la red es escasa o nula. Preferentemente, se requiere una conexión regular con el sistema de gestión de datos para prolongar regularmente la autenticación limitada en el tiempo del aparato de comunicación.

Según una forma de realización preferida, el aparato de comunicación comprende un equipo de control que controla una transmisión de los datos de autenticación por medio de los datos de validez. Por consiguiente, no se envían datos de autenticación a un dispositivo de acceso si el usuario se encuentra en un intervalo de validez no permitido.

De acuerdo con la invención, el aparato de comunicación realiza automáticamente una solicitud al sistema de gestión de datos para la autorización del usuario en un intervalo de tiempo predeterminado. Preferentemente, el aparato de comunicación se comunica con el sistema de gestión de datos a través de un primer canal de comunicación. Por motivos de seguridad, es útil que el aparato de comunicación se comunique con el sistema de gestión de datos a intervalos regulares para actualizar la autorización del usuario. De acuerdo con la invención, los datos de autenticación se borran si no hay autorización. Esto tiene lugar mediante el equipo de control del aparato de comunicación o el software. En consecuencia, los datos de autenticación ya no se transmiten al dispositivo de acceso. El usuario recibe preferentemente un aviso de revocación de la autorización de acceso.

El intervalo de tiempo predeterminado puede ser el periodo de validez predeterminado (plazo del contrato) o un intervalo de tiempo más pequeño. Este intervalo de tiempo se puede predeterminar globalmente o especificar para grupos específicos de datos de autenticación, por ejemplo, para regiones específicas.

Preferentemente, pasado aproximadamente el 50 % del intervalo de tiempo o periodo de validez predeterminado, se intenta la solicitud de autorización del usuario. Si no se puede establecer una conexión con el sistema de gestión de datos, se realizarán más intentos.

Poco antes del tiempo restante, se presenta al usuario el mensaje correspondiente de que se requiere una conexión al sistema de gestión de datos.

Preferentemente, incluso después de que haya expirado el intervalo de tiempo o el periodo de validez, se intenta contactar periódicamente con el sistema de gestión de datos y renovar los datos de autenticación. Además, al usuario se le presenta un aviso correspondiente. Según una forma de realización preferida, el usuario puede darse de baja utilizando

el aparato de comunicación. Preferentemente, a este respecto, la unidad de control del aparato de comunicación borra los datos de autenticación en el aparato de comunicación. Preferentemente, el sistema de gestión de datos sigue asignando los datos de autenticación dados de baja al usuario, de modo que permanece visible un historial del usuario.

Según una forma de realización preferida, el usuario puede bloquear los datos de autenticación asignados a un aparato de comunicación. Preferentemente, cuando el aparato de comunicación se usa por primera vez después del bloqueo, el dispositivo de acceso usa el segundo canal de comunicación para enviar comandos para sobrescribir los datos de autenticación en el aparato de comunicación. Esta función es necesaria cuando el aparato de comunicación ya no está autorizado para acceder al dispositivo de acceso. Este puede ser el caso, por ejemplo, si el aparato de comunicación se pierde o se vende, o si el propietario se muda a otra área. El aparato de comunicación se puede identificar basándose en los datos de identificación de aparato. Por lo tanto, los datos de autenticación asociados se configuran como perdidos en el sistema de gestión de datos.

Si el aparato de comunicación se pone en contacto con el sistema de gestión de datos, el periodo de validez preferentemente ya no se prolonga y el usuario recibe la información adecuada de que este aparato de comunicación ya no se puede utilizar.

Según una forma de realización preferida, la comunicación por medio del segundo canal de comunicación es una comunicación HCE (Host based Card Emulation) (emulación de tarjeta basada en hospedador)). Android ofrece comunicación HCE desde la versión 4.4. La comunicación HCE se basa en las normas ISO 14443-A e ISO 7816. Es decir, el hardware NFC del dispositivo de acceso siempre envía un comando, al que el aparato de comunicación responde con una "respuesta". El contacto se establece preferentemente entre el dispositivo de acceso y el aparato de comunicación utilizando un comando de Select Aid ISO 7816. Cualquier dato puede entonces intercambiarse en los pares de comando-respuesta.

Después del comando Select AID, el aparato de comunicación responde con la versión (más reciente) del protocolo HCE admitido en el aparato de comunicación así como el UID (virtual) del aparato de comunicación. El sistema Android procesa el comando Select Aid y se inicia la aplicación que se ha registrado para la ayuda dada en el sistema. Si varias aplicaciones se han registrado para la misma ayuda, se le preguntará al usuario a qué aplicación debe dirigirse.

Preferentemente, el dispositivo de acceso pregunta activamente al aparato de comunicación por medio de una orden de comando si está presente una respuesta "Response" en el aparato de comunicación. Esto significa que el aparato de comunicación no puede iniciar una transferencia de datos durante la comunicación HCE. Preferentemente, el aparato de comunicación responde inmediatamente.

Preferentemente el intercambio de datos entre el aparato de comunicación y el dispositivo de acceso consiste en una transmisión de comandos de aplicación, que consisten en una orden y datos a transmitir.

Según otra forma de realización preferida, se usa un protocolo de transporte para la transmisión de comandos de aplicación, mediante lo cual los comandos de aplicación se dividen en uno o varios segmentos y se transmiten en función del tamaño de datos del comando de aplicación.

Según otro aspecto de la invención, el objetivo se consigue mediante un sistema de acceso para llevar a cabo un procedimiento según una de las formas de realización anteriores.

El sistema de acceso puede presentar una o varias características ya mencionadas para el procedimiento. En consecuencia, todas las características del procedimiento también deben considerarse divulgadas con respecto al sistema de acceso.

Otras ventajas, objetivos y propiedades de la presente invención se explican en base a la siguiente descripción de las figuras adjuntas. Los componentes similares pueden presentar los mismos números de referencia en las distintas formas de realización.

En las figuras muestran:

la figura 1 una vista general del sistema de acceso;

las figuras 2a a 2isecuencia a modo de ejemplo de una pantalla en el teléfono inteligente cuando la aplicación se inicia por primera vez.

En la figura 1 se muestra una vista general del sistema de acceso (1). En el sistema de acceso tiene lugar un procedimiento para manejar un sistema de acceso (1) con un dispositivo de acceso (2), en particular para un contenedor de basura (3), que comprende las siguientes etapas:

a. registrar al usuario (4) mediante un aparato de comunicación (5) en un sistema de gestión de datos (6) por medio de un primer canal de comunicación (7);
b. transmitir un conjunto de datos mediante el sistema de gestión de datos (6) a través del primer canal de comunicación (7) al aparato de comunicación (5), en donde el conjunto de datos comprende datos de autenticación y datos de validez;
c. iniciar un intercambio de datos a través de un segundo canal de comunicación (8) entre el aparato de comunicación (5) y el dispositivo de acceso (2), en donde al menos los datos de autenticación se transmiten al dispositivo de acceso (2), en donde el segundo canal de comunicación (8) es una conexión inalámbrica, y
d. comprobar los datos de autenticación mediante un equipo de control (9) del dispositivo de acceso (2) para una autorización del usuario;

en donde el registro tiene lugar una vez y los datos de autenticación autorizan el acceso al dispositivo de acceso (2) en un intervalo de validez predeterminado.

El aparato de comunicación (5) comprende un equipo de control (10) que controla una transmisión de los datos de autenticación por medio de los datos de validez.

En adelante, el término aplicación (App) también puede entenderse como el equipo de control (10) del aparato de comunicación (5), dado que la aplicación está instalada en este equipo de control (10) y el equipo de control realiza las acciones correspondientes.

No es necesario iniciar la aplicación (10) manualmente para abrir la esclusa. La aplicación (10) se abrirá automáticamente y desaparecerá nuevamente después de un tiempo establecido.

Todos los propietarios de claves registrados se gestionan en el sistema de gestión de datos o en el portal web. ID de sus teléfonos inteligentes (en lo sucesivo, también ID de clave (virtuales)) corresponden a ID de etiquetas usadas anteriormente. Estos también se pueden desactivar/bloquear allí de nuevo. Esto puede ser necesario cuando un usuario cambia o pierde su teléfono inteligente o ya no está autorizado para acceder a esclusas de basura. En este caso, el ID de la aplicación (10) se introduce en una lista prohibida (lista negra).

Otra información necesaria que aún tiene que asignarse a las claves son características de identificación del teléfono inteligente (5) (ID de dispositivo única y nombre del teléfono inteligente) y funciones que tienen que implementarse en el portal web.

Las aplicaciones tienen que ser distribuidas. Para ello, la aplicación se almacena en una tienda web (15) (por ejemplo, Google Play Store).

ID de clave (virtuales) para la aplicación de teléfono inteligente (10) se pueden generar, por ejemplo, mediante un generador de claves que garantice la unicidad de ID de clave generados. Para poder utilizar un teléfono inteligente (5) como clave de acceso para el dispositivo de acceso (2), se requiere un proceso de registro y autenticación y una asignación de la identificación del usuario (por regla general el número de contrato). Para ello, se tienen realizar preparativos en el sistema de gestión de datos (6) y por parte del municipio o la empresa de eliminación de basuras (12):

- Importación de datos de usuario (13) (nombre, dirección, número de contrato, código de región, código de registro, código de registro 2).
- Carta de información (14) con código de registro y código de registro 2 a los usuarios (4) por parte del municipio o empresa de eliminación de basuras (12). El número de contrato también debe ser visible en esta carta. El número de contrato y el código de registro asociado también deben incluirse en la carta como código QR para simplificar el registro con la aplicación (10). Para registrarse en la aplicación (10), únicamente ha de escanearse el código QR. La carta de información (14) contiene además una descripción de dónde se puede descargar la aplicación (recomendación: incluir un segundo código QR con un enlace a la aplicación en la tienda web (15) y cómo se lleva a cabo el proceso de registro.

Con base en la carta de información (14), el usuario (4) sabe en qué tienda de aplicaciones (15) puede comprar la aplicación de llave virtual para el dispositivo de acceso y cómo puede registrar el teléfono inteligente (5).

Después de descargar e instalar la aplicación, se le pedirá al usuario (4) que introduzca su número de contrato junto con el código de registro recibido. Esta información se transmite al sistema de gestión de datos a través de una conexión segura (https) junto con una identificación única del teléfono inteligente y el nombre del dispositivo, donde se verifica su coincidencia. Para aumentar la seguridad, se toman las siguientes precauciones adicionales:

- El proceso de registro se cancela cuando el código de registro se ha introducido incorrectamente varias veces. Después tiene que solicitar una nueva activación del código de registro desde el centro de soporte.
- Se debe especificar el número máximo de llaves permitidas (5) para cada ID de usuario (número de contrato). Una llave (5) es una etiqueta, tarjeta o teléfono inteligente (5) con una aplicación instalada y NFC activado.

Con ello se autentica al usuario (4). Este número máximo de llaves permitidas (5) solo cuenta las llaves (5) asignadas al usuario (4) con el estado "activo". Por lo tanto, a un usuario (4) se le puede asignar cualquier número de llaves (5) en un estado diferente (por ejemplo, "perdido"). Cada teléfono inteligente registrado (5) se cuenta a este respecto como una llave (5) en el portal web y no se pueden registrar más teléfonos inteligentes (5) con un código de registro una vez que se haya alcanzado el número máximo de llaves (activas) (5).

Si el número de contrato y el código de registro coinciden y si aún no se ha alcanzado el número máximo de llaves activas, la información relevante para el acceso se transmite a la aplicación (10), incluidas las identificaciones de clave únicas (que el portal web utiliza del conjunto de ID de llaves virtuales disponibles seleccionados y activos), código de región, tipo llave, datos de cifrado y validez. Esta información se transmite parcialmente a la aplicación (10) dentro de un registro de datos de autenticación que se crea por el sistema de gestión de datos. Solo entonces es posible abrir un dispositivo de acceso con el mismo código de región con el teléfono inteligente (5).

Para abrir una esclusa de basura (2) a través de un teléfono inteligente (5), únicamente se tiene que activar NFC. La aplicación se ejecuta en segundo plano y, por lo tanto, no es necesario reiniciarla específicamente para una eliminación de basura. Basta con encender el teléfono inteligente (5). En función de la forma de realización, el teléfono inteligente (5) se puede mantener de inmediato (es decir, sin más acción en la esclusa de basura (2) o presionando un botón) dentro del intervalo de detección de la antena. Tan pronto como el teléfono inteligente (5) ha sido reconocido por la esclusa de basura (2), aparece un mensaje en la pantalla del teléfono inteligente. La esclusa se abre si el código de región y el estado de llave coinciden.

Durante el uso de un teléfono inteligente (5) en una esclusa (2), el teléfono inteligente (5) no necesariamente tiene que tener una conexión GSM. Esto garantiza que el dispositivo de acceso pueda abrirse incluso si la cobertura de la red es escasa o nula en la ubicación de la esclusa de basura (2). No obstante, se requiere una conexión regular con el sistema de gestión de datos (6) para prolongar regularmente la autenticación temporal de la aplicación (10). La aplicación de llave virtual (10) regenera automáticamente los datos de autenticación en segundo plano. Esto significa que las aplicaciones de llave virtual (10) se pueden volver a desactivar a través del portal cuando los usuarios (4) cambian o pierden su teléfono inteligente (5) o ya no están autorizados a acceder al mismo por otros motivos.

Una aplicación de llave virtual (10) también se puede desactivar a través de la función de lista de bloqueo ya existente de una esclusa de basura (2). Para ello, el estado de ID de llave del teléfono inteligente (5) en cuestión tiene que configurarse como "perdido" en el sistema de gestión de datos (6). Una vez enviada la lista de bloqueados a las esclusas de basura (2) correspondientes, la función de apertura de la aplicación (10) se desactiva al detectarse la pérdida de una llave.

Por motivos de seguridad, está previsto de acuerdo con la invención que la aplicación (10) contacte con el portal a intervalos regulares (periodo de validez) y obtenga autorización para abrir esclusas (2) nuevamente.

Si la ID de llave de un teléfono inteligente (5) ya no está marcada como activa en el portal web (6), el teléfono inteligente (5) ya no recibe esta autorización, por lo tanto, una apertura de la esclusa (2) con este teléfono inteligente (5) con este número de identificación unívoco ya no es posible. Cuando se revoca la autorización para abrir, la aplicación (10) borra los datos de autenticación para que ya se transmitan (no se puedan transmitir) a una esclusa de basura (2). El usuario (4) recibe una notificación de que se ha revocado la autorización para abrir las esclusas de basura (2).

A Una secuencia de ejemplo de una pantalla en el teléfono inteligente cuando la aplicación (10) se inicia por primera vez se muestra a continuación con referencia a las figuras 2a a 2i. Si la aplicación no está (o ya no está) registrada, se le pedirá al usuario que se registre:
Figura 2a: El dispositivo no se ha comunicadónaún. Después, aparece la pantalla para desbloquear el dispositivo. Se introduce el número de contrato y el código de registro. El sistema de gestión de datos (6) comprueba si los datos son válidos. Se proporciona un escáner de código QR para que el usuario no tenga que introducir la información requerida a mano (Figura 2b).

Cada vez que se inicia la aplicación, se comprueba si NFC está activa. Si NFC no está activa, se informa al usuario y se le da la oportunidad de cambiar a configuración (Figura 2c). Si la aplicación ya está registrada (y NFC activa), se muestra la pantalla que se muestra en la figura 2d: Si el periodo de validez de los datos de autenticación ha expirado, se muestra el mensaje correspondiente. Si los datos de autenticación se han borrado, el usuario será informado de este hecho y luego se le pedirá que se registre nuevamente. Después de registrar con éxito la aplicación, se muestra un asistente de ayuda de acuerdo con las figuras 2e a 2g, que describe brevemente cómo usar la aplicación.

Según el estado, durante el proceso de apertura se muestra un mensaje de éxito de acuerdo con la figura 2h o una pantalla con un mensaje de error de acuerdo con la figura 2i.

Lista de referencias

1 sistema de acceso
2 dispositivo de acceso
3 contenedor de basura
4 usuario
5 aparato de comunicación
6 sistema de gestión de datos
7 primer canal de comunicación
8 segundo canal de comunicación
9 equipo de control del dispositivo de acceso
10 equipo de control del aparato de comunicación

REIVINDICACIONES

1. Procedimiento para manejar un sistema de acceso (1) con un dispositivo de acceso (2), en particular para un contenedor de basura (3), que comprende las siguientes etapas:

a. registrar al usuario (4) mediante un aparato de comunicación (5) en un sistema de gestión de datos (6) por medio de un primer canal de comunicación (7);
b. transmitir un conjunto de datos mediante el sistema de gestión de datos (6) a través del primer canal de comunicación (7) al aparato de comunicación (5), en donde el conjunto de datos comprende datos de autenticación y datos de validez;
c. iniciar un intercambio de datos a través de un segundo canal de comunicación (8) entre el aparato de comunicación (5) y el dispositivo de acceso (2), en donde al menos los datos de autenticación se transmiten al dispositivo de acceso (2), en donde el segundo canal de comunicación (8) es una conexión inalámbrica;
d. comprobar los datos de autenticación mediante un equipo de control (9) del dispositivo de acceso (2) para una autorización del usuario;

en donde el registro tiene lugar una vez y los datos de autenticación autorizan el acceso al dispositivo de acceso (2) en un intervalo de validez predeterminado, en donde en el momento del intercambio de datos a través del segundo canal de comunicación (8) no tiene que existir conexión alguna del aparato de comunicación (5) con el sistema de gestión de datos (6) por medio del primer canal de comunicación (7), caracterizado por que el aparato de comunicación (5), en un intervalo de tiempo predeterminado, lleva a cabo automáticamente una solicitud de la autorización del usuario (4) en el sistema de gestión de datos (6), en donde, en ausencia de autorización, los datos de autenticación del aparato de comunicación (5) se borran y dejan de transmitirse al dispositivo de acceso (2).

2. Procedimiento para manejar un sistema de acceso (1) según la reivindicación 1,

caracterizado por que
el aparato de comunicación (5) es un aparato de procesamiento de datos portátil, por ejemplo un teléfono móvil, un teléfono inteligente, una tableta o un ordenador portátil, en donde el aparato de comunicación (5) presenta un equipo de control (10) en el que está instalado un software, por medio del cual se permite el registro del usuario en el sistema de gestión de datos y/o por medio del cual se puede controlar el intercambio de datos a través de un segundo canal de comunicación (8) entre el aparato de comunicación (5) y el dispositivo de acceso (2).

3. Procedimiento para manejar un sistema de acceso (1) según la reivindicación 1 o 2,

caracterizado por que
el primer canal de comunicación (7) es una conexión móvil y la conexión inalámbrica del segundo canal de comunicación es una conexión NFC o una conexión RFID, en donde la conexión móvil es, por ejemplo, una conexión GSM o una conexión UMTS o una conexión GPRS o una conexión LTE.

4. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores,

caracterizado por que
en la etapa a) datos de identificación de usuario, datos de identificación de aparato del aparato de comunicación y un código de registro, que es proporcionado por un operador, se transmiten al sistema de gestión de datos (6) mediante el aparato de comunicación (5), en donde los datos de identificación de usuario y el código de registro se introducen por lectura por medio de un escáner QR del aparato de comunicación (5).

5. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores,

caracterizado por que
durante el uso del aparato de comunicación (5) en el dispositivo de acceso (2), el aparato de comunicación (5) no tiene conexión con el sistema de gestión de datos (6) a través del primer canal de comunicación (7).

6. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores,

caracterizado por que
el aparato de comunicación (5) comprende un equipo de control (10) que controla una transmisión de los datos de autenticación por medio de los datos de validez.

7. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores,

caracterizado por que
una baja del registro se puede llevar a cabo por el usuario (4) por medio del aparato de comunicación (5), en donde el equipo de control (10) del aparato de comunicación (5) borra los datos de autenticación en el aparato de

comunicación (5), en donde el sistema de gestión de datos (6) continúa asignando al usuario (6) los datos de autenticación dados de baja.

8. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores,

caracterizado por que
los datos de autenticación asignados a un aparato de comunicación (5) pueden ser bloqueados por el usuario (4), en donde durante el primer uso del aparato de comunicación (5) después del bloqueo, el dispositivo de acceso (2), por medio del segundo canal de comunicación (8) envía comandos para sobrescribir los datos de autenticación en el aparato de comunicación (5).

9. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores,

caracterizado por que
la comunicación por medio del segundo canal de comunicación (8) es una comunicación HCE (Host based Card Emulation) (emulación de tarjeta basada en hospedador)), en donde se establece contacto entre el dispositivo de acceso (2) y el aparato de comunicación (5) mediante un comando Select Aid ISO 7816.

10. Procedimiento para manejar un sistema de acceso (1) según la reivindicación 9,

caracterizado por que
el dispositivo de acceso (2) solicita activamente en el aparato de comunicación (5) por medio de una orden de comando si hay una respuesta en el aparato de comunicación (5), teniendo lugar inmediatamente la respuesta del aparato de comunicación (5).

11. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores 9 o 10,

caracterizado por que
el intercambio de datos entre el aparato de comunicación (5) y el dispositivo de acceso (2) consiste en una transmisión de comandos de aplicación, que consisten en una orden y datos a transmitir.

12. Procedimiento para manejar un sistema de acceso (1) según una de las reivindicaciones anteriores 9 a 11,

caracterizado por que
para la transmisión de comandos de aplicación se usa un protocolo de transporte, mediante lo cual los comandos de aplicación se dividen en uno o más segmentos y se transmiten en función del tamaño de datos del comando de aplicación.

13. Sistema de acceso (1), que comprende un dispositivo de acceso (2) con un dispositivo de control (9), un aparato de comunicación (5), un sistema de gestión de datos (6) y un primer (7) y un segundo canal de comunicación (8), en donde el sistema de acceso está configurado para llevar a cabo un procedimiento según una de las reivindicaciones anteriores.

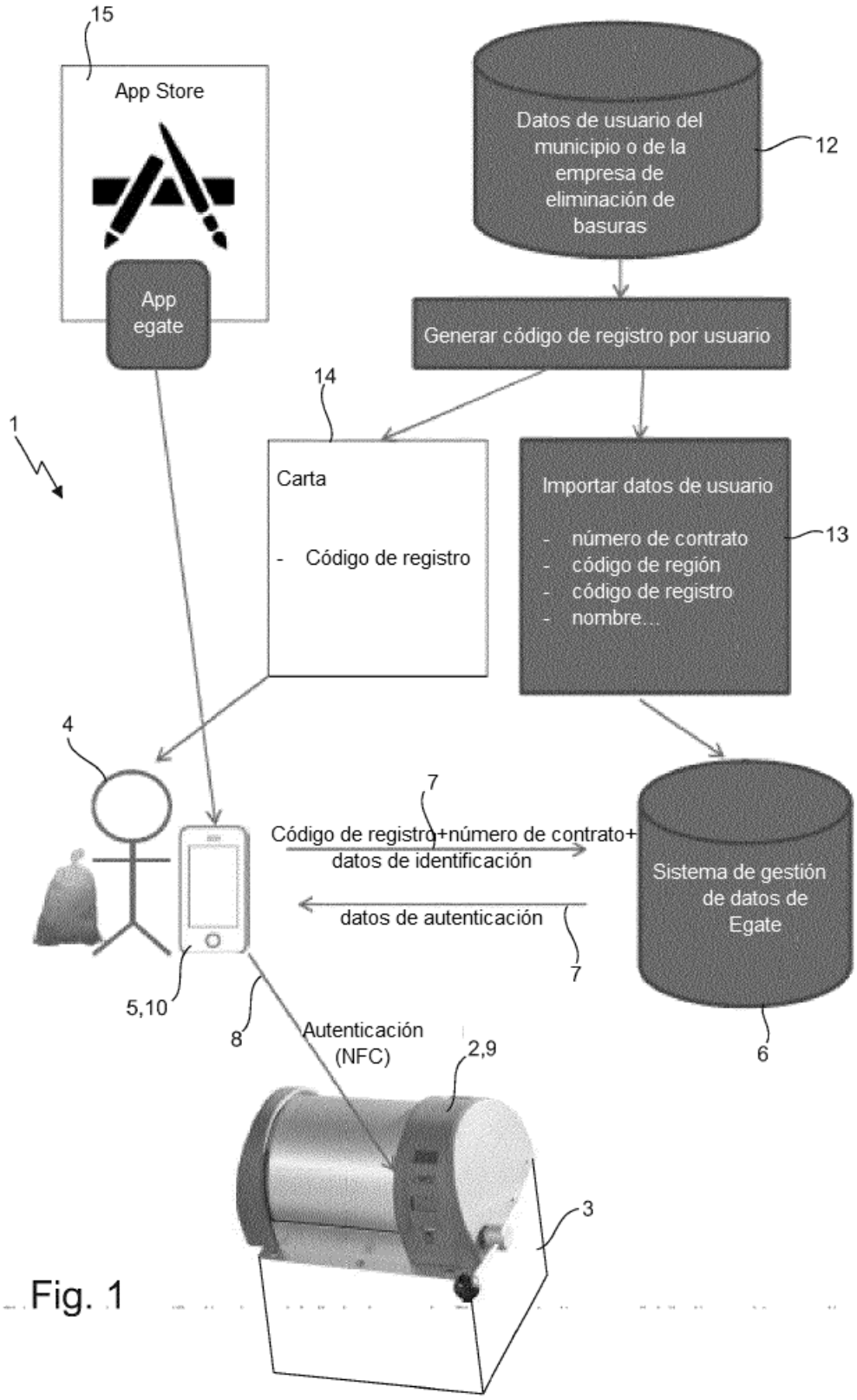
15
App Store
App egate
Datos de usuario del municipio o de la empresa de eliminación de basuras
12
Generar código de registro por usuario
14
1
Carta
- Código de registro
Importar datos de usuario
- número de contrato
- código de región
- código de registro
- nombre...
13
4
7
Código de registro+número de contrato+ datos de identificación
datos de autenticación
7
Sistema de gestión de datos de Egate
6
5,10
8
Autenticación (NFC)
2,9
3

Fig. 1

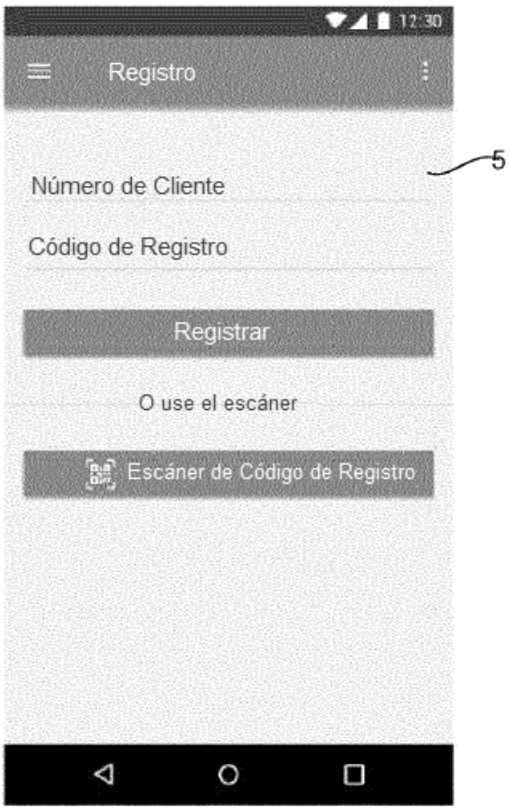
12:30
Registro
5
Número de Cliente
Código de Registro
Registrar
O use el escáner
Escáner de Código de Registro

Fig. 2a

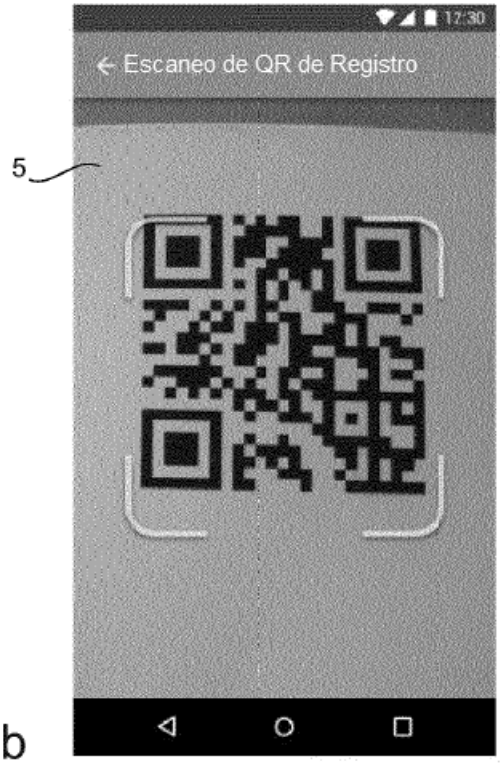
17:30
← Escaneo de QR de Registro
5

Fig. 2b

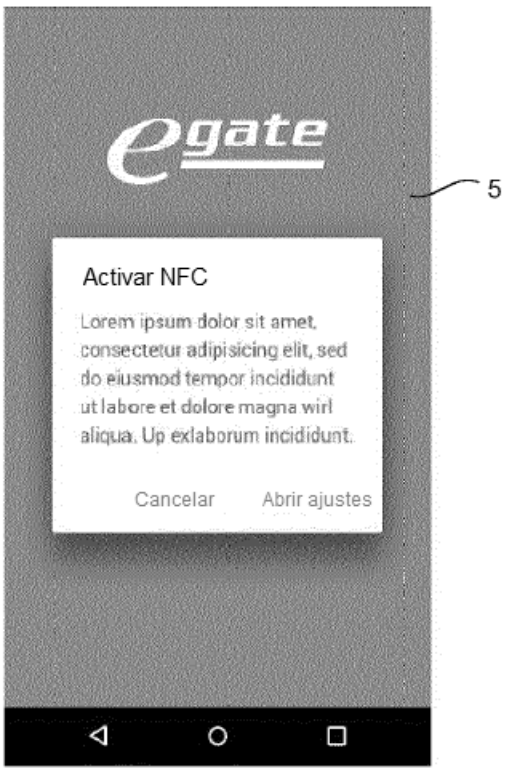
egate
5
Activar NFC
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna wirl aliqua. Up exlaborum incididunt.
Cancelar
Abrir ajustes

Fig. 2c


12:30
eGate smartKey
5
Mantenga su dispositivo cerca de eGate
Pulse primero el botón conectar en eGate

Fig. 2d

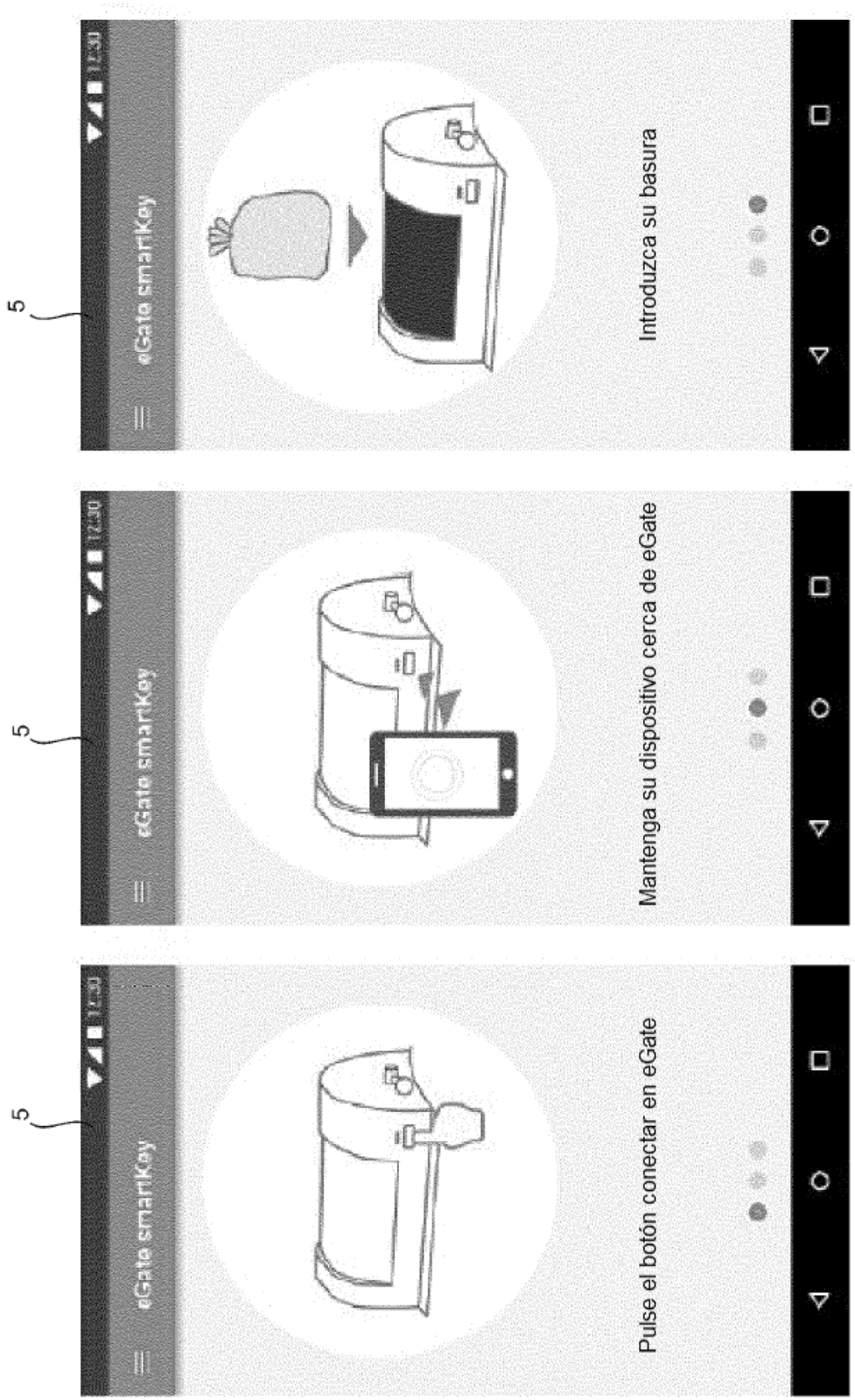

Fig. 2e

Fig. 2f

Fig. 2g


12:30
eGate smartKey
5
eGate abierta
Introduzca su basura

Fig. 2h


12:30
eGate smartKey
5
Acceso denegado
No se puede abrir eGate
Inténtelo de nuevo o póngase en contacto con el servicio de asistencia

Fig. 2i