

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 890 960**

51 Int. Cl.:

G07C 9/00

(2010.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **10.11.2017** **E 17201190 (0)**

97 Fecha y número de publicación de la concesión europea: **04.08.2021** **EP 3483841**

54 Título: **Sistema de gestión de listas negras electrónicas y procedimiento de control de autorización para el uso de un recipiente de residuos**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
25.01.2022

73 Titular/es:

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

72 Inventor/es:

ALTENHOFER, HERBERT

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 890 960 T3

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

DESCRIPCIÓN

Sistema de gestión de listas negras electrónicas y procedimiento de control de autorización para el uso de un recipiente de residuos

La invención se refiere a un sistema electrónico de gestión de listas negras y a un procedimiento para verificar la autorización para el uso de un contenedor de basura. El procedimiento se caracteriza porque las entradas dentro de una lista de exclusión se priorizan de acuerdo con la probabilidad de un intento de inicio de sesión, cuanto más rápido y con menos esfuerzo de procesamiento de datos, se puede evitar el uso de un contenedor de basura por usuarios no autorizados.

Para la eliminación de los desechos domésticos, a menudo se proporcionan contenedores de basura a gran escala, que son utilizados por varios hogares. Dichos contenedores de basura pueden pertenecer, por ejemplo, a una comunidad de viviendas o también a un municipio. Como regla general, solo los usuarios registrados deben tener acceso a dichos contenedores de basura, por lo que se puede bloquear el acceso, por ejemplo, si no se pagan los costos de eliminación. Este tipo de acceso se puede implementar utilizando una amplia variedad de sistemas electrónicos. Se sabe por el estado de la técnica, por ejemplo, que se asigna un código de identificación a un usuario. Este código de identificación se almacena, por ejemplo, en un chip o una tarjeta, que el usuario lleva dentro o sobre (por ejemplo, cuando se utiliza tecnología de transmisión por radio del código de identificación (por ejemplo, mediante RFID)) en un lector compatible para identificarse. El correspondiente proceso de autenticación se lleva a cabo por una unidad de control local en el contenedor de basura o por un servidor central que está conectado a la unidad de control local del contenedor de basura. Después de la autenticación exitosa y la asignación del código de identificación al grupo autorizado, el contenedor de basura se abre temporalmente y el usuario puede deshacerse de su basura.

En el caso de los sistemas de acceso electrónico en los que se utilizan claves (de escritura) con un ID único (por ejemplo, transpondedores con chips RFID), puede ser necesario bloquear una o más de estas claves. La necesidad surge, por ejemplo, si se pierde una clave y se debe evitar que personas no autorizadas sigan utilizándola en el sistema de acceso. Si bien es ventajoso para los sistemas de acceso electrónico, a los que solo unos pocos participantes deberían tener acceso (como un cubo de basura residual para una casa de una o dos familias), solo este grupo de residentes puede identificarse como personas autorizadas utilizando una lista de códigos de identificación aprobados ("lista blanca"), la gestión de listas con un gran número de entradas de códigos de identificación aprobados, por ejemplo, para residuos de vidrio central, ropa vieja o contenedores de residuos verdes, a los que, por ejemplo, todos los residentes de una ciudad tienen acceso, significa un gran esfuerzo de procesamiento de datos. Si un sistema de acceso tiene una gran cantidad de claves, es posible que se requiera una gran cantidad de códigos de identificación, que deben almacenarse en cada sistema de acceso. Esto tiene varias desventajas, en particular a) se requiere una gran cantidad de memoria para los códigos de identificación, b) hay un gran volumen de datos cuando se transmiten las listas de códigos de identificación grandes, c) actualizaciones frecuentes de las listas de códigos de identificación de todos los sistemas de acceso en un área son necesarios y) las listas de códigos de identificación grandes dan como resultado tiempos de búsqueda prolongados, lo que resulta en tiempos de espera más prolongados debido a la identificación del usuario antes de que se otorgue cualquier autorización de acceso. Para tales sistemas, por lo tanto, es aconsejable reemplazar la lista de códigos de identificación autorizados de acceso por una lista comparativamente corta de códigos de identificación para los que se excluye el acceso al sistema de eliminación ("lista negra").

Para dicha lista negra, se debe almacenar una lista con las entradas de bloqueo (códigos de identificación bloqueados) en el área de memoria del sistema de acceso, que se busca cuando se autentica una clave. En algunos de los casos mencionados con anterioridad, en los que, por ejemplo, casi todos los vecinos de una ciudad tienen acceso al sistema de disposición, estas listas negras también pueden llegar a ser muy largas en poco tiempo por diversos motivos, de modo que las desventajas que se plantean con anterioridad en cuanto a la lista blanca también pueden ocurrir aquí.

Dicho sistema de acceso también debe ser informado de muchos códigos de identificación bloqueados en un corto período de tiempo y almacenarse en la lista negra, por ejemplo, cuando los residentes se mudan, no pagan tarifas o pierden claves o tarjetas. También en este caso, el resultado es que a) se necesitaría una gran cantidad de memoria para las entradas de bloqueo, b) se requiere un gran volumen de datos para la transmisión de las listas negras grandes, c) actualizaciones frecuentes de las listas negras de todos los sistemas de acceso en un área son necesarios y d) las listas negras grandes pueden resultar en tiempos de búsqueda prolongados. Las listas negras para los sistemas de acceso suelen ser generadas por el proveedor de servicios de eliminación local utilizando un sistema de gestión de datos adecuado. El documento KR20150051931 A divulga un sistema de contenedores de basura en el que se utiliza una lista negra en el curso de los controles de acceso, que es administrada por un servidor de administración de listas negras, en donde el servidor reenvía la información de la lista negra recibida de un contenedor de basura a los otros contenedores de basura cuya lista negra aún no contiene esta información.

Por lo tanto, la presente invención se basa en el objeto de proporcionar un sistema y un procedimiento para la gestión de datos que permita el procesamiento eficaz y, en particular, más rápido de una lista negra para el control de autorización electrónica para el uso de un contenedor de basura.

Este objeto se logra mediante un sistema electrónico de gestión de listas negras para un control de autorización para el uso de un contenedor de basura de acuerdo con la reivindicación 1 y mediante un procedimiento para la gestión de datos de una lista negra en un sistema de acceso para un control electrónico de autorización para el uso de un contenedor de basura de acuerdo con la reivindicación 8.

En el lado del dispositivo, se prevé así que el sistema de gestión de listas negras electrónicas para un control de autorización para el uso de un contenedor de basura comprende un sistema de gestión de datos y un gran número de sistemas de acceso para un control de autorización electrónico para el uso de un contenedor de basura individual asignado a cada sistema de acceso individual. Los sistemas de acceso se pueden activar mediante un gran número de claves, cada una de las cuales puede asignarse a un usuario o grupo de usuarios. Tanto el sistema de gestión de datos como cada uno de los sistemas de acceso tienen una interfaz de comunicación mediante la cual se pueden intercambiar datos entre el sistema de gestión de datos y cada sistema de acceso individual. Además, cada sistema de acceso tiene un dispositivo de memoria para crear y almacenar una lista de las claves utilizadas en este sistema de acceso en un período determinado, así como medios para transmitir esta lista al sistema de gestión de datos por medio de la interfaz de comunicación. Preferiblemente, un sistema de acceso de este tipo también tiene un dispositivo de registro de tiempo, de modo que se puede agregar un sello de tiempo a cada intento de acceso por medio de una clave. El sello de tiempo se almacena preferiblemente con la entrada respectiva del intento de acceso de la clave utilizada en este sistema de acceso. En particular, se prefiere que el sello de tiempo se transmita al sistema de gestión de datos junto con la entrada respectiva del intento de acceso de la clave utilizada en este sistema de acceso. Como resultado, el sistema de gestión de datos, que preferiblemente tiene una mayor capacidad de almacenamiento y tiene una mayor potencia de cálculo que el sistema de acceso, puede archivar los datos en los intentos de acceso con claves específicas junto con la marca de tiempo. Esto asegura la utilidad de los datos determinados por el sistema de acceso a través de intentos de acceso durante un largo período de tiempo.

El sistema de gestión de datos tiene dispositivos para crear una lista negra para el sistema de acceso de un contenedor de basura, en donde el sistema de gestión de datos está configurado para utilizar un algoritmo de priorización para priorizar las entradas en la lista negra al crear la lista negra. El algoritmo de priorización también tiene en cuenta al menos la característica del último uso de una clave no autorizada en el sistema de acceso del contenedor de basura respectivo. Al utilizar la función del último uso de una clave no autorizada en el sistema de acceso del contenedor de basura respectivo, se puede evitar que las claves que se hayan destruido o perdido y no se hayan encontrado ya no tengan que mantenerse en la lista negra y, por lo tanto, no bloquee ningún espacio de almacenamiento. Si se volviera a encontrar una clave perdida, si ya no estuviera en la lista negra debido al largo período de inactividad, se podría volver a utilizar porque no estaba en la lista negra, pero se reutilizaría la próxima vez que se actualizara debido al uso renovado de la lista negra, se pueden agregar nuevamente y, debido a su uso reciente, se enumeran con una prioridad correspondientemente alta en la lista negra.

Cada sistema de acceso cuenta además con un dispositivo de memoria para el almacenamiento de la lista negra, que se transmite desde el sistema de gestión de datos y desde este al respectivo sistema de acceso, para el contenedor de basura asignado a este sistema de acceso. Como resultado, la lista negra también está disponible para este sistema de acceso después de la transferencia de datos para comparar con las claves que preguntan sobre el uso del contenedor de basura asignado. Por tanto, no es necesaria una conexión de datos existente al sistema de gestión de datos. Además, cada sistema de acceso comprende un dispositivo de procesamiento de datos y un dispositivo de control para otorgar o denegar el acceso al contenedor de basura asignado al sistema de acceso para un usuario asignado a la clave, siendo una denegación de acceso una consecuencia de una comparación exitosa de la clave con las entradas contenidas en la lista negra. El dispositivo de procesamiento de datos compara una clave que pregunta sobre el uso del contenedor de basura asignado al sistema de acceso con las entradas contenidas en la lista negra. Si la clave no está excluida del uso del contenedor de basura asignado al sistema de acceso, el dispositivo de control puede otorgar acceso al contenedor de basura.

Preferiblemente, se asigna exactamente un contenedor de basura a cada sistema de acceso. Así, un sistema de acceso puede controlar el acceso al contenedor de basura asignado.

El control de autorización para el uso de un contenedor de basura se realiza mediante claves. Se asigna una clave a cada usuario o grupo de usuarios. Tal clave puede ser un número de identificación (ID), por ejemplo. A este respecto, cabe señalar que el término número de identificación no se limita a números, sino que se utiliza en general para cualquier cadena de caracteres que permita la asignación a un usuario. Este ID puede ser, por ejemplo, un PIN (número de identificación personal (código PIN)) que debe introducir el usuario o puede almacenarse en un soporte de datos que el sistema de acceso puede leer. Tal soporte de datos legible es preferiblemente un soporte de datos que se selecciona de un grupo que incluye una tarjeta con chip, una etiqueta RFID, un teléfono móvil, una tableta, una computadora portátil, un dedo (huella digital), la cara (escaneo facial) e incluye un ojo (escaneo del iris). Debido al menor gasto en equipo y al menor consumo de energía, una tarjeta con chip, una etiqueta RFID o un teléfono móvil (por ejemplo, a través de NFC (Near Field Communication) o Bluetooth) son especialmente preferidos para identificar a un usuario. Se prefiere especialmente la tecnología NFC porque casi todos los teléfonos inteligentes ahora son compatibles con esta tecnología y, por lo tanto, existe una gran variedad de dispositivos de identificación correspondientes.

Por lo general, un sistema de acceso para monitorear y controlar el acceso al contenedor de basura requiere energía, generalmente energía eléctrica. Dado que los contenedores de basura se encuentran a menudo en espacios públicos, en muchos casos no hay acceso a una red eléctrica. Por tanto, se prefiere un suministro de energía descentralizado. Esto podría hacerse, por ejemplo, mediante baterías, acumuladores o energía solar. También son posibles combinaciones de estos o suplementos con otras fuentes de energía. Por ejemplo, es concebible que la energía requerida se obtenga de la energía solar y se almacene en acumuladores. Una batería como fuente de energía de emergencia, si no se dispone de otras fuentes de energía, también sería concebible (independientemente y en combinación con otras fuentes de energía).

Dado que, como se mencionó con anterioridad, el acceso a la red eléctrica a menudo no está disponible en tales sistemas, el uso de sistemas de procesamiento de datos que consumen mucha energía solo es posible hasta un grado muy limitado en el control y monitoreo del acceso al contenedor de basura. Los límites asociados en el rendimiento de los sistemas de procesamiento de datos conducen al retraso mencionado al principio al verificar las autorizaciones de acceso de una lista con un gran número de entradas. Para evitar o al menos reducir tales retrasos, es necesario definir un número máximo de entradas en una lista a partir de la cual se determina la autorización de acceso. Por lo tanto, se descarta una lista blanca (como se describe al principio), especialmente en sistemas con un gran número de usuarios autorizados. Los sistemas con un gran número de usuarios autorizados se pueden gestionar de forma especialmente eficaz mediante una lista negra o entradas de lista negra. Dado que las listas con entradas en la lista negra también pueden superar un tamaño crítico con el tiempo, también se debe especificar un número máximo de entradas en la lista negra para garantizar que el sistema de acceso pueda procesarlas rápidamente.

Preferiblemente está previsto que un sistema de acceso tenga un dispositivo de bloqueo con un dispositivo de bloqueo. El dispositivo de bloqueo se puede utilizar, por ejemplo, para tirar basura en el contenedor de basura. Solo cuando se desbloquea un dispositivo de bloqueo, el usuario (o el propio sistema de acceso) puede abrir un acceso a la cerradura. En una realización preferida, el dispositivo de control emite una señal de liberación para desbloquear el dispositivo de bloqueo. Sin embargo, esto solo tiene lugar si la comparación de la clave con las entradas en la lista negra en el dispositivo de procesamiento de datos es negativa.

Debido a la frecuente disposición de los contenedores de basura en espacios públicos de libre acceso, el acceso a una red de datos por cable a menudo no está disponible o es muy limitado. Por lo tanto, en una realización preferida, la interfaz de comunicación para intercambiar los datos entre el sistema de gestión de datos y cada sistema de acceso individual es una interfaz de comunicación adecuada para la comunicación inalámbrica. Debido a la gran cobertura de la red, se prefiere particularmente un dispositivo de comunicación por radio móvil, que se selecciona de manera particularmente preferida de un grupo que comprende un dispositivo de comunicación por radio móvil GSM, UMTS, GPRS y LTE. Como alternativa o además de esto, también sería concebible una conexión WLAN (conexión a través de una red de área local inalámbrica), ya que una red de este tipo ahora también está disponible en muchas ciudades. Como alternativa a la transmisión inalámbrica de datos, también sería posible la transmisión mediante un soporte de datos (por ejemplo, una tarjeta de memoria o un lápiz de memoria (por ejemplo, lápiz USB). Esto podría realizarse, por ejemplo, cuando o mientras se vacía el contenedor de basura. Dado que la transmisión de datos a menudo no es crítica en cuanto al tiempo y, por ejemplo, durante la noche o durante períodos de poco uso de la red de transmisión, la velocidad de transmisión de datos tiene una importancia secundaria, particularmente en el caso de la transmisión de datos inalámbrica.

En otra realización preferida, un sistema de acceso y/o un contenedor de basura tiene un dispositivo de localización, mediante el cual se puede determinar la ubicación actual del contenedor de basura. Además, el dispositivo de localización utiliza preferiblemente un sistema de navegación por satélite global para determinar la ubicación actual. Este se selecciona de forma particularmente preferida de un grupo que comprende NAVSTAR GPS (Sistema de posicionamiento global), GLONASS (Sistema de navegación por satélite global), Galileo y Beidou. La ubicación actual se puede transmitir preferiblemente al sistema de gestión de datos, preferiblemente a través de la interfaz de comunicación ya mencionada con anterioridad. La determinación y transmisión de la ubicación actual del contenedor de basura al sistema de gestión de datos tiene la ventaja de que se puede localizar fácilmente un contenedor de basura que se ha retirado de la ubicación prevista, por ejemplo, debido a vandalismo o robo. Además, también se pueden determinar los otros contenedores de basura ubicados en las proximidades de este contenedor de basura, que, como se muestra más adelante, se pueden tener en cuenta para la determinación de las listas negras.

El algoritmo de priorización es de particular importancia para una asignación eficiente de claves individuales a las listas negras de contenedores de basura individuales o el sistema de acceso respectivo asignado a este contenedor de basura. Mediante el uso de este algoritmo de priorización, se puede generar una lista negra, que por un lado es lo más corta posible, pero por otro lado contiene tantas entradas de cerradura que se evita o al menos se minimiza el uso no autorizado del contenedor de basura respectivo con un alto grado de probabilidad.

En una realización preferida, el algoritmo de priorización comprende reglas de cálculo que mapean al menos una característica seleccionada de un grupo que comprende

- la frecuencia con la que se utiliza una clave no autorizada en el sistema de acceso del contenedor de basura respectivo,

- el último uso de una clave no autorizada en un sistema de acceso de otro contenedor de basura, que está ubicado geográficamente a una distancia predefinida del respectivo contenedor de basura,
- la frecuencia del último uso de una clave no autorizada en un sistema de acceso de otro contenedor de basura, que está ubicado geográficamente a una distancia predefinida del respectivo contenedor de basura,
- el importe de una factura pendiente para el usuario asignado a esta clave y
- la distribución geográfica del uso de una clave no autorizada en un sistema de acceso de otros contenedores de basura.

Al mapear una o más de estas características en las reglas de cálculo del algoritmo de priorización, se pueden prever varios escenarios concebibles de uso indebido de una clave y se pueden preparar los sistemas de acceso correspondientes de los contenedores de basura respectivos para el posible uso indebido de una clave incluyéndola en la respectiva lista negra.

Si, por ejemplo, la frecuencia de uso de una clave no autorizada en un sistema de acceso de un determinado contenedor de basura es muy alta, es muy probable que el usuario al que (ahora) ya no se le permite usarla todavía desea utilizar este contenedor de basura con un alto grado de probabilidad. Al priorizar su clave en consecuencia en la lista negra creada individualmente para este contenedor de basura, se puede evitar el uso indebido.

También existe una alta probabilidad de que un usuario que ya no está autorizado a acceder intente utilizar contenedores de basura en las proximidades del contenedor de basura previamente preferido y utilizado con mayor frecuencia. Dado que (como se mencionó con anterioridad) la posición (actual) de los contenedores de basura individuales se puede conocer, monitorear o determinar si es necesario, los contenedores de basura se pueden determinar rápidamente que están ubicados geográficamente a una distancia predefinida del contenedor de basura utilizado por última vez por el usuario para ser excluido. Si el último uso de una clave no autorizada en un sistema de acceso de otro contenedor de basura que está ubicado geográficamente a una distancia predefinida (pequeña) del contenedor de basura respectivo no fue hace mucho tiempo, esto también puede resultar en una alta priorización de esta clave en un usuario no utilizado previamente por este usuario contenedor de basura usado.

Si la frecuencia del último uso de una clave no autorizada en un sistema de acceso de otro contenedor de basura que se encuentra geográficamente a una distancia predefinida (pequeña) del respectivo contenedor de basura es muy alta, esto también puede indicar que el usuario no autorizado que se encuentra en esta área está frecuentemente activo y con una alta probabilidad también podría usar este recipiente de desechos en el futuro. Una alta priorización de esta clave en este contenedor de basura también conduce a un rechazo de uso incluso antes del primer intento de uso.

También sería concebible basar la priorización en la distribución geográfica del uso de una clave (ahora) no (ya no) autorizada en un sistema de acceso de otros contenedores de basura. Por ejemplo, si un usuario ha utilizado con anterioridad principalmente dos contenedores de basura diferentes (por ejemplo, en el hogar y en el trabajo), teniendo en cuenta la distribución geográfica del uso de estos contenedores de basura, los contenedores de basura que se encuentran en el medio (por ejemplo, en el área de las carreteras principales) también podría excluirse del uso por parte de este usuario incluyéndolo con una prioridad correspondientemente alta en las respectivas listas negras del sistema de acceso de los contenedores de basura allí colocados.

Otro posible criterio para una alta priorización podría ser el monto de una factura pendiente del usuario asignado a esta clave. Con una priorización tan alta, a los usuarios que no han pagado facturas durante un largo período de tiempo también se les puede prohibir el uso de contenedores de basura que se encuentran muy lejos de los contenedores de basura que se utilizan habitualmente y en su lista negra debido a la gran distancia de estos usuarios morosos debido a los criterios descritos con anterioridad, de lo contrario, no se llevaría a cabo.

En una realización preferida, el sistema de gestión de listas negras electrónicas se caracteriza porque al menos uno de los sistemas de acceso, preferiblemente una pluralidad de sistemas de acceso, más preferiblemente todos los sistemas de acceso, tiene un dispositivo para excluir una clave de todos los sistemas de acceso de los sistemas de gestión de listas negras electrónicas. Tal dispositivo para excluir una clave de todos los sistemas de acceso del sistema de gestión de listas negras electrónicas podría ser, en una realización preferida, por ejemplo, un dispositivo para retirar la clave o para borrar, sobrescribir o reproducir de otro modo un número de identificación almacenado en la clave inutilizable.

Si, por ejemplo, se utilizan tarjetas con chip para la identificación, el sistema de acceso podría conservarlas después de (posiblemente múltiples) intentos de acceso no autorizados o rechazados. Cuando se vacía el contenedor de basura, el personal operativo también podría retirar la tarjeta con chip retenida del sistema de acceso y así sacarla de circulación.

En el caso de identificación a través de una clave que no tiene que estar físicamente en contacto con el sistema de acceso (por ejemplo, una etiqueta RFID, un teléfono móvil u otro sistema sin contacto), normalmente no es posible la retención, por lo que la clave podría quedar inutilizable si se elimina, se sobrescribe o de cualquier otra forma. Sería concebible, por ejemplo, que todas las claves de un área contengan un prefijo uniforme, que las clasifica como pertenecientes a esta área (por ejemplo, una ciudad, un distrito, un lugar o un distrito). Si este prefijo se borra, se

sobrescribe o se inutiliza de alguna otra manera, los sistemas de acceso de esta área ya no reaccionan a esta clave, por lo que el uso de esta clave queda excluido para toda el área.

Si un sistema de acceso detecta el ID de una clave no autorizada durante el proceso de autenticación, el sistema de acceso puede destruir los datos de la clave no autorizada mediante acceso de escritura o al menos modificarlos de tal manera que su función sea perturbada. Esto significa que el proceso de autenticación de la clave no autorizada ya no funciona en ningún otro sistema de acceso.

En este contexto, se prefiere particularmente si la información sobre una clave destruida se transmite desde el sistema de acceso destructivo al sistema de gestión de datos. Esto significa que la entrada de bloqueo para esta clave se puede eliminar de todas las listas negras, lo que crea espacio libre para otra clave no autorizada.

En cuanto al procedimiento, el objeto en el que se basa la invención se logra mediante un procedimiento de gestión de datos de una lista negra en un sistema de acceso para el control de autorización electrónica para el uso de un contenedor de basura, con los siguientes pasos

- a. definición de un número máximo de entradas en la lista negra,
- b. transmisión de las claves utilizadas con anterioridad en el sistema de acceso de cada contenedor de basura individual desde un gran número de contenedores de basura a un sistema de gestión de datos.
- c. si aún no se ha alcanzado el número máximo de entradas de la lista negra: Inclusión de la clave no autorizada en la lista negra y transferencia de la lista negra a los sistemas de acceso de todos los contenedores de basura por el sistema de gestión de datos, o si el número máximo de entradas de la lista negra ha sido alcanzado:
- d. establecimiento de un algoritmo de priorización para priorizar entradas en una lista negra para el sistema de acceso de un contenedor de basura, teniendo en cuenta el algoritmo de priorización al menos también la característica del último uso de una clave no autorizada en el sistema de acceso del respectivo contenedor de basura,
- e. creación de una clasificación de prioridad individual de todas las claves inaccesibles para el sistema de acceso de cada contenedor de basura definido individualmente por el sistema de gestión de datos,
- f. inclusión de las claves inaccesibles comenzando con la clave con la mayor prioridad en orden descendente de prioridad en la lista negra individual del sistema de acceso de cada contenedor de basura definido individualmente hasta que el sistema de gestión de datos alcance el número máximo de entradas en la lista negra,
- g. transmisión de la lista negra individual al sistema de acceso de cada contenedor de basura definido individualmente y
- h. concesión o denegación de acceso a un contenedor de basura definido de acuerdo con la clave almacenada en la lista negra individual del sistema de acceso del respectivo contenedor de basura definido.

Se determina un número máximo de entradas en la lista negra, como ya se mostró con anterioridad, preferiblemente dependiendo del rendimiento del sistema de acceso respectivo. Dado que una pequeña cantidad de entradas en la lista negra permite un procesamiento de datos relativamente rápido incluso con sistemas de acceso comparativamente ineficientes, se prefiere un número máximo bajo de entradas en la lista negra. El número máximo de entradas de la lista negra es particularmente preferiblemente 5000 entradas, más preferiblemente 2^{12} entradas, más preferiblemente 2^{11} entradas, en particular preferiblemente 2^{10} entradas, más preferiblemente 1000 entradas, más preferiblemente 2^5 entradas, más preferiblemente 500 entradas, en particular preferiblemente con 400 entradas, más preferiblemente con 2^8 entradas, más preferiblemente con 2^7 entradas y en particular preferiblemente con 100 entradas. Con un número tan reducido de entradas, con el hardware actual, incluso con un consumo de energía extremadamente bajo, el sistema de acceso puede realizar una comparación con una lista negra casi sin demoras perceptibles para el usuario. La definición de un número máximo de entradas en la lista negra no tiene que realizarse cada vez que se crea una nueva lista negra. Por lo tanto, mantener un valor previamente definido de un número máximo de entradas de la lista negra también debe entenderse como la definición de un número máximo de entradas de la lista negra para los fines de esta invención.

Como se muestra arriba, el último (y/o frecuente) uso de una clave en este o en un contenedor de basura geográficamente cercano es importante para evaluar la probabilidad de uso inadecuado de un contenedor de basura. Por lo tanto, está previsto que (preferiblemente de forma periódica) las claves utilizadas previamente en el sistema de acceso de cada contenedor de basura individual de un gran número de contenedores de basura se transmitan a un sistema de gestión de datos en un período de tiempo especificado.

Si aún no se ha alcanzado el número máximo de entradas en la lista negra, todas las claves no autorizadas se pueden agregar a la lista negra. Esta lista negra es la misma para los sistemas de acceso de todos los contenedores de basura, de modo que el sistema de gestión de datos pueda transmitirla a todos los sistemas de acceso. Sin embargo, a más tardar cuando se haya alcanzado el número máximo de entradas de la lista negra, se prevé que se establezca un algoritmo de priorización para la priorización de entradas en una lista negra para el sistema de acceso de un contenedor de basura. El algoritmo de priorización también tiene en cuenta al menos la característica del último uso de una clave no autorizada en el sistema de acceso del contenedor de basura respectivo. Dado que todos los intentos de acceder a los contenedores de basura individuales se tienen en cuenta para crear las listas negras, las listas negras individuales son necesarias. A cada contenedor de basura se le asigna así una lista negra individual, que al menos en una buena aproximación refleja la probabilidad de uso indebido de una clave precisamente en este contenedor de basura.

El sistema de gestión de datos crea así una secuencia de priorización individual de todas las claves no autorizadas para el sistema de acceso de cada contenedor de basura definido individualmente. Con base en este orden de prioridad, comenzando con la clave con la prioridad más alta en orden descendente de prioridad, se genera una lista negra individual para el sistema de acceso de cada contenedor de basura definido individualmente, y cada entrada se transfiere a la lista negra individual hasta el número máximo de las entradas de la lista negra se alcanza es. Alternativamente, si el número de entradas según el orden de prioridad excede el número máximo de entradas de la lista negra, la entrada con la prioridad más baja podría eliminarse en este orden hasta que el número de claves en este orden de prioridad individual corresponda al número máximo de entradas permitido de listas negras. Las claves que es poco probable que se utilicen precisamente en este contenedor de basura no se incluyen en la lista negra asignada a este contenedor de basura si su ubicación en el orden de prioridad excede el número máximo de entradas de la lista.

Las listas negras individuales generadas de esta manera para un sistema de acceso específico se transfieren luego al sistema de acceso del contenedor de basura respectivo. Por lo tanto, la lista negra con las claves más probablemente mal utilizadas para este contenedor de basura está disponible para el sistema de acceso allí en el futuro incluso sin una conexión de datos existente y permite la evaluación de una autorización de acceso para una clave específica.

Si un usuario intenta acceder al contenedor de basura con una determinada clave, el sistema de acceso puede otorgar o denegar el acceso de acuerdo con la clave almacenada en la lista negra individual para el contenedor de basura respectivo. Por lo tanto, solo es posible que los usuarios utilicen este contenedor de basura cuya clave no está contenida en la lista negra individual almacenada en el sistema de acceso de este contenedor de basura.

La expresión "lista negra individual" debe entenderse en el sentido de esta invención de tal manera que se determine una lista negra por separado para cada contenedor de basura o cada grupo de contenedores de basura. Sin embargo, es perfectamente concebible que las listas negras determinadas por separado también puedan ser idénticas para diferentes contenedores de basura. Tales listas negras idénticas también deben entenderse como listas negras individuales en el sentido de esta invención.

Como ya se describió con anterioridad en el lado del dispositivo, también es ventajoso en términos del procedimiento si el algoritmo de priorización continúa teniendo en cuenta características que se seleccionan de un grupo que comprende

- la frecuencia de uso de una clave no autorizada en el sistema de acceso del contenedor de basura respectivo,
- el último uso de una clave no autorizada en un sistema de acceso de otro contenedor de basura, que está ubicado geográficamente a una distancia predefinida del respectivo contenedor de basura,
- la frecuencia del último uso de una clave no autorizada en un sistema de acceso de otro contenedor de basura, que está ubicado geográficamente a una distancia predefinida del respectivo contenedor de basura,
- el importe de una factura pendiente para el usuario asignado a esta clave y
- incluye la distribución geográfica del uso de una clave no autorizada en un sistema de acceso de otros contenedores de basura.

Si se excede un número especificado de intentos de acceso rechazados de una clave que no está autorizada para el acceso, la clave se excluye ventajosamente del uso posterior por parte del sistema de acceso. Esto se puede hacer preferiblemente mediante el sistema de acceso retirando la clave o borrando, sobrescribiendo o haciendo de otro modo inutilizable un número de identificación almacenado en la clave.

También se prefiere un procedimiento en el que el procesamiento de datos por el sistema de gestión de datos se lleva a cabo por separado del contenedor de basura respectivo. Esto tiene la ventaja de que el procesamiento de datos por parte del sistema de gestión de datos puede tener lugar de forma centralizada para todos los contenedores de basura. Preferiblemente se lleva a cabo en un lugar donde se dispone de energía suficiente para el funcionamiento de un potente sistema de gestión de datos y, opcionalmente, también un sistema de archivo. Por lo tanto, la información sobre intentos de acceso no autorizados también se puede archivar durante un largo período de tiempo y/o cuando se vuelve a utilizar una clave que no se ha utilizado durante un largo período de tiempo, los datos de uso asociados con esta clave se pueden volver a utilizar.

Los datos se pueden transmitir, por ejemplo, cuando se vacía el contenedor de basura respectivo. Sin embargo, se prefiere una variante alternativa del procedimiento en la que la transmisión de datos entre un sistema de acceso de un contenedor de basura y el sistema de gestión de datos se realiza de forma inalámbrica. Esto también permite intercambiar datos entre dos vacíos, por ejemplo, si se espera un uso inadecuado de un contenedor de basura en un futuro próximo. Con la transmisión inalámbrica de datos, no es necesario enviar a un empleado a actualizar la lista negra de un contenedor de basura.

Se prefiere particularmente una variante del procedimiento en la que la transmisión de datos entre un sistema de acceso de un contenedor de basura y el sistema de gestión de datos se realiza mediante una conexión de radio móvil, que se selecciona preferiblemente de un grupo que comprende una conexión GSM, una conexión UMTS, una conexión GPRS y una conexión LTE.

En una variante preferida del procedimiento, los pasos b, e, f y g antes mencionados se llevan a cabo repitiéndose periódicamente, teniendo lugar la repetición preferiblemente en un intervalo que se selecciona de un grupo que es diario, semanal, mensual, trimestral, semestral o incluye repetición anual. De esta forma, se puede garantizar un estado de datos actualizado en los sistemas de acceso de todos los contenedores de basura. Por supuesto, también sería concebible utilizar el sistema y procedimiento descritos para controlar el acceso a los contenedores de basura de diferentes tipos de basura, como basura residual, papel, botellas, metal, madera, residuos verdes, basura peligrosa, sobras de medicamentos o contenedores de plástico.

Otras ventajas, objetivos y propiedades de la presente invención se explican con referencia a la siguiente descripción de las Figuras adjuntas. Los componentes del mismo tipo pueden tener los mismos símbolos de referencia en las diversas realizaciones.

En las Figuras se muestra:

Fig. 1 muestra una descripción general de un sistema de gestión de listas negras electrónicas para el control de autorización para el uso de un contenedor de basura;
Fig. 2 muestra un diagrama esquemático del sistema de gestión de listas negras electrónicas para el control de autorización para el uso de un contenedor de basura según una realización;
Fig. 3 muestra una representación ejemplar para la creación de una clasificación de prioridad y una lista negra individual resultante de la misma.

La Figura 1 muestra una vista general del sistema de gestión de listas negras electrónicas para el control de autorización para el uso de un contenedor de basura. Este sistema incluye un sistema de gestión de datos (1). Esta puede disponerse en el centro y preferiblemente está separada espacialmente de cada uno de los contenedores de basura (2.1, 2.2, 2.n). Cada uno de los contenedores de basura (2.1, 2.2, 2.n) está conectado a un sistema de acceso (3.1, 3.2, 3.n) que controla el acceso al respectivo contenedor de basura (2.1, 2.2, 2.n). Para ello, se proporciona un dispositivo de bloqueo o dispositivo de transferencia (4.1, 4.2, 4.n), que puede bloquearse mediante un dispositivo de bloqueo (5.1, 5.2, 5.n). Si el dispositivo de bloqueo (4.1, 4.2, 4.n) está bloqueado, el acceso al contenedor de basura respectivo (2.1, 2.2, 2.n) está bloqueado y la basura no puede ser arrojada a este contenedor de basura (2.1, 2.2, 2.n).

El sistema de acceso (3.1, 3.2, 3.n) basado en una clave asignada al usuario, por ejemplo, un ID (6.1, 6.2, 6.n). Para ello, el sistema de acceso (3.1, 3.2, 3.n) cuenta con un dispositivo de procesamiento de datos (7.1, 7.2, 7.n) y un dispositivo de almacenamiento (8.1, 8.n). Una lista negra individual asignada al contenedor de basura respectivo (2.1, 2.2, 2.n) se almacena en el dispositivo de almacenamiento respectivo (8.1, 8.n) y contiene aquellas claves (6.1, 7.2, 6.n) a las que se accede a este el contenedor de basura (2.1, 2.2, 2.n) debe ser rechazado.

Si, por el contrario, el usuario utiliza una clave (6.1, 7.2, 6.n) que no está incluida en la lista negra individual de este contenedor de basura (2.1, 2.2, n), también se utiliza una clave en los sistemas de acceso (3.1, 3.2, 3.n) contenidos en el dispositivo de control 9.1, 9.2, 9.n) desbloquean el dispositivo de bloqueo (5.1, 5.2, 5.n) y el acceso al dispositivo de bloqueo (4.1, 4.2, 4. n) se libera para que el usuario pueda tirar la basura a través del dispositivo de bloqueo (4.1, 4.2, 4.n) en el contenedor de basura (2.1, 2.2, 2.n).

La clave (6.1, 7.2, 6.n) del usuario es leída por el sistema de acceso respectivo (3.1, 3.2, 3.n) a través de una interfaz de comunicación (10.1, 10.2, 10.n). La clave (6.1, 7.2, 6.n) puede ser, por ejemplo, una tarjeta con chip, una etiqueta RFID o un teléfono móvil. La interfaz de comunicación (10.1, 10.2, 10.n) es preferiblemente adecuada para la comunicación inalámbrica.

En la realización mostrada, el sistema de acceso (3.1, 3.2, 3.n) de cada contenedor de basura (2.1, 2.2, 2.n) también tiene un dispositivo de localización (11.1, 11.2, 11.n) y un dispositivo de grabación (12.1, 12.2, 12.n). La ubicación actual del contenedor de basura respectivo (2.1, 2.n) se puede determinar mediante el dispositivo de localización (11.1, 11.2, 11.n), por ejemplo, mediante NAVSTAR GPS (Sistema de posicionamiento global), GLONASS (Global Sistema de navegación por satélite), Galileo o Beidou o una combinación de diferentes sistemas se pueden determinar. El dispositivo de registro de tiempo (12.1, 12.2, 12.n) puede usarse para asignar un sello de tiempo único a cada intento de uso por parte de un usuario, de modo que cada intento de uso para cada contenedor de basura (2.1, 2.2, 2.n) se puede documentar tanto en términos de ubicación como de tiempo. Además de esto o como alternativa, la ubicación del sistema de acceso también podría determinarse en el momento de la puesta en servicio o el mantenimiento en el sitio utilizando una herramienta de servicio (por ejemplo, una aplicación de teléfono inteligente) que puede recopilar datos de GPS y los datos de ubicación del sistema de acceso o el contenedor de basura almacenado directamente en el sistema de gestión de datos o en el sistema de acceso. El sistema de acceso puede luego transmitir estos datos al sistema de gestión de datos por radio.

La interfaz de comunicación (10.1, 10.2, 10.n) también se utiliza para transferir datos hacia y desde el sistema de gestión de datos (1). Para ello, la interfaz de comunicación (10.1, 10.2, 10.n) tiene preferiblemente un canal de comunicación separado. Este se diferencia preferentemente de aquél mediante el cual se lee la clave de un usuario. Los dos canales de comunicación de la interfaz de comunicación (10.1, 10.2, 10.n) también pueden diseñarse como

subunidades separadas que están separadas espacialmente entre sí en o sobre el contenedor de basura (2.1, 2.2, 2.n) y/o se disponga el sistema de acceso (3.1, 3.2, 3. n).

La interfaz de comunicación (10.1, 10.2, 10.n) está diseñada preferiblemente para la comunicación inalámbrica con el sistema de gestión de datos (1). Esto tiene la ventaja de que el personal operativo no tiene que intercambiar los datos manualmente (por ejemplo, mediante una memoria USB). Se utiliza preferiblemente una conexión de radio móvil para el intercambio de datos entre la interfaz de comunicación (10.1, 10.2, 10.n) y el sistema de gestión de datos (1).

La Figura 2 muestra un diagrama esquemático del sistema de gestión de listas negras electrónicas para el control de autorización para el uso de un contenedor de basura según una realización. Como se muestra en este diagrama esquemático, se crea una lista de todas las claves no autorizadas en un paso (21). Si esta lista es tan larga que debe esperarse una autenticación retardada de las claves en el sistema de acceso (3.1, 3.2, 3.n) de los respectivos contenedores de basura (2.1, 2.2, 2.n), en el paso 22 se debe esperar un número máximo x de entradas por lista negra. Si este número x es menor que el número de todas las entradas en la lista de claves inaccesibles, es necesario en el paso (23) definir criterios mediante los cuales un algoritmo de priorización puede determinar un orden de prioridad de claves inaccesibles.

Para permitir un control de acceso efectivo a un contenedor de basura específico (por ejemplo, 2.1 de una gran cantidad de contenedores de basura (2.1, 2.2, 2.n), todos los intentos de acceder a todas las claves en cada sistema de acceso (3.1, 3.2, 3. n) del sistema reconocido y almacenado en el paso (25) durante un período especificado en el dispositivo de almacenamiento del sistema de acceso (3.1, 3.2, 3. n).

En el paso (26), los datos almacenados en uno o más sistemas de acceso (3.1, 3.2, 3.n) se transmiten al sistema de gestión de datos (1) mediante intentos de acceso. Esta transmisión puede tener lugar a intervalos regulares, iniciada por el usuario o cuando se excede (por ejemplo, > 75%, preferiblemente > 80%, en particular preferiblemente > 90%) una utilización de memoria especificada del dispositivo de almacenamiento (8.1, 8.2, 8.n) del respectivo sistema de acceso (3.1, 3.2, 3.n). Después de la transferencia, los datos transferidos se pueden almacenar y archivar en el sistema de gestión de datos (1), de modo que el dispositivo de almacenamiento (8.1, 8.2, 8.n) del sistema de acceso respectivo (3.1, 3.2, 3.n) sea puede vaciarse para almacenar nuevos datos sobre los intentos de acceso.

Si los datos se han transferido al sistema de gestión de datos (1) mediante intentos de acceso, en el paso (27) se puede crear un orden de prioridad para las claves inaccesibles para cada sistema de acceso (3.1, 3.2, 3.n) en la base del algoritmo de priorización definido previamente (ver paso 23). Dado que los datos sobre los intentos de acceso a los distintos contenedores de basura (2.1, 2.2, 2.n) difieren, existe un orden de priorización individual para cada contenedor de basura (2.1, 2.2, 2.n) basado en los intentos de acceso y un algoritmo de priorización subyacente. En particular, en el caso de sistemas más grandes con un gran número de contenedores de basura (2.1, 2.2, 2.n), es de esperar una cantidad comparativamente grande de esfuerzo informático.

Sobre la base del orden de priorización individual, se genera una lista negra individual para cada contenedor de basura (2.1, 2.2, 2.n) en el paso (28). Esto se limita a un número de x entradas para mantener el procesamiento de datos por parte del sistema de acceso (3.1, 3.2, 3.n) en el sitio lo más bajo posible. Las entradas cuya posición en el orden de prioridad supere el número x no se incluyen en la lista negra.

Una vez generadas las listas negras, la lista negra individual se transmite al sistema de acceso respectivo (3.1, 3.2, 3.n) en el paso (29). Dependiendo del ancho de banda disponible de la red de transmisión, esto se puede hacer de manera conjunta para todas las listas negras y sistemas de acceso (3.1, 3.2, 3.n) o solo para sistemas de acceso individuales (3.1, 3.2, 3.n) o un grupo de sistemas de acceso (3.1, 3.2, 3.n).

Después de la transferencia, la respectiva lista negra está disponible en el sistema de acceso correspondiente (3.1, 3.2, 3.n) para evaluar la autorización de acceso de los usuarios de una clave específica. Si la clave con la que un usuario solicita acceso al contenedor de basura (2.1, 2.2, 2.n) está contenida en la lista negra del sistema de acceso (3.1, 3.2, 3.n) de este contenedor de basura (2.1, 2.2, 2.n), se deniega el acceso al contenedor de basura (2.1, 2.2, 2.n) y el dispositivo de bloqueo (5.1, 5.2, 5.n) permanece bloqueado.

La Figura 3 muestra un ejemplo de representación para la creación de una clasificación de prioridad y una lista negra individual resultante de la misma. En el área de la izquierda (columnas 1 y 2), se muestran todos los datos transmitidos al sistema de gestión de datos (1) sobre intentos de acceso a un contenedor de basura específico durante un período de varios días consecutivos. Los respectivos registros de datos contienen un sello de tiempo y una identificación de clave. Los registros de datos contienen intentos de acceso mediante claves autorizadas y (en este caso dos) claves no autorizadas (ID de clave resaltada en negrita).

En el sistema de gestión de datos (1) se almacenan determinados factores de ponderación para cada segmento de tiempo (en este caso A, B, C y D) (en este caso 10, 8, 6 y 4). En el ejemplo mostrado, el factor de ponderación asignado al segmento de tiempo respectivo se asigna a cada uno de los intentos de acceso con una clave no permitida. El producto del número de intentos de acceso por segmento de tiempo y el factor de ponderación respectivo da como resultado un valor para cada segmento de tiempo y cada clave no permitida. Si suma los valores para cada clave

individualmente, la suma da como resultado un valor de ponderación que se puede usar para priorizar. En el presente ejemplo, la clave A8E1AD06 tiene una prioridad más alta que la clave 5CA3DA03, que solo llegó a un total de 28, debido al total de 46 determinadas.

- 5 Los valores de ponderación que se muestran aquí como ejemplos tienen únicamente fines ilustrativos. La ponderación se puede adaptar a las necesidades respectivas. El sistema también se puede optimizar utilizando otros factores de ponderación. Por ejemplo, entre claves que no están autorizadas para el acceso, el motivo de la retirada de la autorización también se puede incluir en la ponderación.
- 10 Si, por ejemplo, se perdió una clave y se perdió otra autorización de acceso debido a que un residente se mudó, una ponderación más alta podría ser ventajosa para la clave perdida debido al usuario poco claro y una mayor probabilidad de uso ilegal, mientras que el residente aún se puede identificar quién se mudó, por lo que aún se pueden reclamar las tarifas de uso del contenedor de basura.
- 15 Además, las marcas de tiempo de las claves no autorizadas que todavía están en uso podrían tener una ponderación mayor que las que ya no se utilizan y/o las marcas de tiempo no autorizadas (por ejemplo, después de perder la clave) tienen una ponderación mayor que las marcas de tiempo autorizadas (es decir, antes de perder la clave).

Lista de signos de referencia

20	1	sistema de gestión de datos
	2.1, 2.2, 2.n	contenedores de basura
	3.1, 3.2, 3.n	sistema de acceso
	4.1, 4.2, 4.n	dispositivo de bloqueo
25	5.1, 5.2, 5.n	dispositivo de bloqueo
	6, 6.1, 6.2, 6.n	clave, ID
	7.1, 7.2, 7.n	dispositivo de procesamiento de datos
	8.1, 8.2, 8.n	dispositivo de almacenamiento
	9.1, 9.2, 9.n	dispositivo de control
30	10.1, 10.2, 10.n	interfaz de comunicación
	11.1, 11.2, 11.n	dispositivo de localización
	12.1, 12.2, 12.n	dispositivo de grabación de tiempo
	21-30	paso

REIVINDICACIONES

1. Sistema electrónico de gestión de listas negras para el control de autorizaciones para el uso de un contenedor de basura (2.1, 2.2, 2.n), en donde el sistema de gestión de listas negras comprende un sistema de gestión de datos (1) y un gran número de sistemas de acceso (3.1, 3.2, 3.n) activables por medio de muchas claves (6) que pueden ser asignadas a un usuario o grupo de usuarios, para un control electrónico de autorización para el uso de un contenedor de basura individual (2.1, 2.2, 2.n) asignado a cada acceso individual (3.1, 3.n), en donde tanto el sistema de gestión de datos (1) como cada uno de los sistemas de acceso (3.1, 3.2, 3.n) presentan una interfaz de comunicación (10.1, 10.2, 10.n), mediante la cual son intercambiables los datos entre el sistema de gestión de datos (1) y cada sistema de acceso individual (3.1, 3.2, 3.n), en donde cada sistema de acceso (3.1, 3.2, 3.n) presenta un dispositivo de almacenamiento (8.1, 8.2, 8.n) para crear y almacenar una lista de las clave utilizada (6, 6.1, 6.2, n) en un período de tiempo establecido en este sistema de acceso (3.1, 3.2, 3.n) y medios para transmitir esta lista mediante la interfaz de comunicación (10.1, 10.2, 10.n) al sistema de gestión de datos (1), y el sistema de gestión de datos (1) presenta dispositivos para la creación de una lista negra para el sistema de acceso (3.1, 3.2, 3.n) de un contenedor de basura (2.1, 2.2, 2.n), en donde

- el sistema de gestión de datos (1) está configurado para utilizar un algoritmo de priorización para priorizar las entradas en la lista negra al crear la lista negra, en donde el algoritmo de priorización al menos también incluye la característica del último uso de una clave (6, 6.1, 6.n) que no estaba autorizado para acceder al sistema de acceso (3.1, 3.2, 3.n) del respectivo contenedor de basura (2.1, 2.n) se tiene en cuenta para que cada uno tenga un ranking de prioridad individual de todos los no autorizados claves (6, 6.1, 6.2, 6.n) con el fin de crear una clasificación de priorización individual de todas las claves (6, 6.1, 6.2, 6.n) no autorizadas para el sistema de acceso (3.1, 3.2, 3.n) de cada contenedor de basura definido individualmente (2.1, 2.2, 2.n) por el sistema de gestión de datos (1), por lo que las claves (6, 6.1, 6.2, 6.n) no autorizadas para el acceso se incluyen en la lista de bloqueo individual por el sistema de gestión de datos (1) empezando por la clave (6, 6.1, 6.2, 6.n) con la mayor priorización en orden descendente de priorización (6, 6.1, 6.2, 6.n), comenzando por la llave (6, 6.1, 6.2, 6.n) con la mayor priorización, en la lista de bloqueo individual del sistema de acceso (3.1, 3.2, 3.n) de cada contenedor de basura definido individualmente (2.1, 2.2, 2.n) en orden descendente de priorización hasta alcanzar el número máximo de entradas de la lista de bloqueo,
- cada sistema de acceso (3.1, 3.2, 3.n) presenta un dispositivo de memoria (8.1, 8.2, 8.n) para almacenar la lista negra creada por el sistema de gestión de datos (1) y transmitida por éste al respectivo sistema de acceso (3.1, 3.2, 3.n) para el contenedor de basura (2.1, 2.n) asignado a este sistema de acceso (3.1, 3.2, 3.n) y cada sistema de acceso (3.1, 3.2, 3.n) comprende un dispositivo de procesamiento de datos (7.1, 7.2, 7.n) y un dispositivo de control (9.1, 9.2, 9.n) para permitir o denegar el acceso al contenedor de basura (2.1, 2.2, 2.n) asignado al sistema de acceso (3.1, 3.2, 3.n) para un usuario asignado a una clave (6, 6.1, 6.2, 6.n), en donde un rechazo de acceso es una consecuencia de una comparación exitosa de la clave (6, 6.1, 6.2, 6.n) con las entradas contenidas en la lista negra individual del sistema de acceso (3.1, 3.2, 3.n) de este contenedor de basura definido (2.1, 2.2, 2.n).

2. Sistema electrónico de gestión de listas negras de acuerdo con la reivindicación 1, caracterizado porque el algoritmo de priorización comprende reglas aritméticas que mapean al menos una característica seleccionada de un grupo formado por:

- la frecuencia de uso de una clave no autorizada (6, 6.1, 6.2, 6.n) en el sistema de acceso (3.1, 3.2, 3.n) del contenedor de basura respectivo (2.1, 2.2, n),
- el último uso de una clave no autorizada (6, 6.1, 6.2, 6.n) en un sistema de acceso (3.1, 3.2, 3.n) de otro contenedor de basura (2.1, 2.2, 2.n), que geográficamente está dispuesto a una distancia predefinida del contenedor de basura respectivo (2.1, 2.2, 2.n),
- la frecuencia del último uso de una clave no autorizada (6, 6.1, 6.2, 6.n) en un sistema de acceso (3.1, 3.2, 3.n) de otro contenedor de basura (2.1, 2.n), que geográficamente está dispuesto a una distancia predefinida del contenedor de basura respectivo (2.1, 2.2, 2.n),
- el importe de una factura pendiente del usuario asignado a esta clave (6, 6.1, 6.2, 6.n) y
- la distribución geográfica del uso de una clave no autorizada (6, 6.n) en un sistema de acceso (3.1, 3.2, n) de otros contenedores de basura (2.1, 2.2, 2.n).

3. Sistema electrónico de gestión de listas negras de acuerdo con la reivindicación 1 o 2, caracterizado porque al menos uno de los sistemas de acceso (3.1, 3.2, 3.n), preferiblemente una pluralidad de sistemas de acceso (3.1, 3.n), más preferiblemente todos sistemas de acceso (3.1, 3.2, 3.n), presentan un dispositivo para excluir una clave (6, 6.1, 6.2, 6.n) a todos los sistemas de acceso (3.1, 3.2, 3.n) del sistema electrónico de gestión de listas negras.

4. Sistema electrónico de gestión de listas negras de acuerdo con reivindicación 3, caracterizado porque el dispositivo de exclusión de una clave (6, 6.2, 6.n) a todos los sistemas de acceso (3.1, 3.2, 3.n) del sistema electrónico de gestión de listas negras es un dispositivo para retirar la clave (6, 6.1, 6.2, 6.n) o para borrar, sobrescribir o inutilizar un número de identificación almacenado en la clave (6, 6.1, 6.2, 6.n).

5. Sistema electrónico de gestión de listas negras de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque la interfaz de comunicación (10.1, 10.2, 10.n) para el intercambio de datos entre el sistema de gestión de datos (1) y cada sistema de acceso individual (3.1, 3.2, 3.n) es una interfaz de comunicación (10.1, 10.2, 10.n) adecuada para la comunicación inalámbrica, que es preferiblemente un dispositivo de comunicación por radio

móvil, que se selecciona de manera particularmente preferida de un grupo que consiste en un dispositivo de comunicación por radio móvil GSM, UMTS, GPRS y LTE.

- 5 6. Sistema electrónico de gestión de listas negras de acuerdo con una de las reivindicaciones anteriores, caracterizado porque un sistema de acceso presenta un dispositivo de puerto (4.1, 4.2, 4.n) con un dispositivo de bloqueo (5.1, 5.2, 5.n), en donde el dispositivo de control (9.1, 9.2, 9.n) emite una señal de liberación para desbloquear el dispositivo de bloqueo (5.1, 5.2, 5.n) cuando la comparación de la clave (6, 6.1, 6.2, 6.n) es negativa con las entradas contenidas en la lista negra en el dispositivo de procesamiento de datos (7.1, 7.2, 7.n).
- 10 7. Sistema electrónico de gestión de listas negras de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque un sistema de acceso (3.1, 3.2, 3.n) y/o un contenedor de basura (2.1, 2.2, 2.n) presenta un dispositivo de localización (11.1, 11.2, 11.n), a través del cual se puede determinar la ubicación actual del contenedor de basura (2.1, 2.2, 2.n), preferiblemente por medio de un sistema global de navegación por satélite, en particular preferiblemente seleccionado de un grupo compuesto por NAVSTAR GPS (Global Sistema de posicionamiento), GLONASS (Sistema global de navegación por satélite), Galileo y Beidou, en donde la ubicación se puede transmitir al sistema de gestión de datos (1), preferiblemente a través de la interfaz de comunicación (10.1, 10.2, 10.n).
- 15 8. Procedimiento para la gestión de datos de una lista negra en un sistema de acceso para un control electrónico de autorización para el uso de un contenedor de basura (2.1, 2.2, 2.n) con los pasos
 - 20 a. definición de un número máximo de entradas en la lista negra,
 - b. transferencia de las claves (6, 6.1, 6.2, 6.n) utilizadas con anterioridad en el sistema de acceso (3.1, 3.2, 3.n) de cada contenedor de basura individual (2.1, 2.n) desde un gran número de contenedores de basura (2.1, 2.2, 2.n) dentro de un período de tiempo especificado a un sistema de gestión de datos (1),
 - 25 c. si aún no se ha alcanzado el número máximo de entradas en la lista negra: inclusión de las claves no autorizadas (6, 6.1, 6.n) en la lista negra y transferencia de la lista negra a los sistemas de acceso (3.1, 3.2, 3.n) de todos contenedores de basura (2.1, 2.2, 2.n) por el sistema de gestión de datos (1), o si se ha alcanzado el número máximo de entradas en la lista negra:
 - d. establecimiento de un algoritmo de priorización para priorizar las entradas en una lista negra para el sistema de acceso (3.1, 3.2, 3.n) de un contenedor de basura (2.1, 2.2, 2.n), tomando en cuenta también el algoritmo de priorización al menos la característica del último uso de una clave no autorizada (6, 6.1, 6.n) en el sistema de acceso del contenedor de basura respectivo (2.1, 2.2, 2.n),
 - 30 e. creación de una clasificación de prioridad individual de todas las claves inaccesibles (6, 6.1, 6.2, 6.n) para el sistema de acceso (3.1, 3.2, 3.n) de cada contenedor de basura definido (2.1, 2.2, 2.n) por el sistema de gestión de datos (1),
 - 35 f. inclusión de las claves inaccesibles (6, 6.1, 6.2, 6.n) comenzando por la clave (6, 6.1, 6.2, 6.n) con la prioridad más alta en orden descendente de prioridad en la lista negra individual del sistema de acceso (3.1, 3.2, 3.n) de cada contenedor de basura definido individualmente (2.1, 2.2, 2.n) hasta que el sistema de gestión de datos (1) alcance el número máximo de entradas en la lista negra,
 - 40 g. transmisión de la lista negra individual al sistema de acceso (3.1, 3.2, 3.n) del contenedor de basura respectivo (2.1, 2.2, 2.n),
 - h. concesión o denegación de acceso a un contenedor de basura definido en función de las claves (6, 6.1, 6.2, 6.n) depositadas en la lista de bloqueo individual del sistema de acceso (3.1, 3.2, 3.n) del respectivo recipiente de residuos definido (2.1, 2.2, 2.n).
- 45 9. Procedimiento de acuerdo con la reivindicación 8, caracterizado porque el algoritmo de priorización tiene en cuenta además características que se seleccionan de un grupo que consiste en
 - la frecuencia de uso de una clave no autorizada (6, 6.1, 6.2, 6.n) en el sistema de acceso (3.1, 3.2, 3.n) del contenedor de basura respectivo (2.1, 2.2, 2.n),
 - el último uso de una clave no autorizada (6, 6.1, 6.2, 6.n) en un sistema de acceso (3.1, 3.2, 3.n) de otro contenedor de basura (2.1, 2.2, 2.n), que geográficamente está dispuesto a una distancia predefinida del contenedor de basura respectivo (2.1, 2.2, 2.n),
 - 50 - la frecuencia del último uso de una clave no autorizada (6, 6.1, 6.2, 6.n) en un sistema de acceso (3.1, 3.2, 3.n) de otro contenedor de basura (2.1, 2.n), que geográficamente está dispuesto a una distancia predefinida del contenedor de basura respectivo (2.1, 2.2, 2.n),
 - 55 - el importe de una factura pendiente del usuario asignado a esta clave (6, 6.1, 6.2, 6.n) y
 - la distribución geográfica del uso de una clave no autorizada (6, 6.n) en un sistema de acceso (3.1, 3.2, 3.n) de otros contenedores de basura (2.1, 2.n).
- 60 10. Procedimiento de acuerdo con la reivindicación 8 o 9, caracterizado porque cuando se excede un número especificado de intentos de acceso rechazados de una clave (6, 6.1, 6.2, 6.n) que no está autorizada para el acceso, la clave (6, 6.1, 6.2, 6.n) está excluida del uso posterior por parte del sistema de acceso (3.1, 3.2, 3.n).
- 65 11. Procedimiento de acuerdo con la reivindicación 10, caracterizado porque el sistema de acceso (3.1, 3.2, 3.n) retira la clave (6.1, 6.2, 6.n) o elimina, sobrescribe o inutiliza de otro modo el número de identificación almacenado en la clave (6, 6.1, 6.2, 6.n).

12. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8 a 11, caracterizado porque el procesamiento de datos por el sistema de gestión de datos (1) se realiza localmente por separado del respectivo contenedor de basura (2.1, 2.2, 2.n).
- 5 13. Procedimiento de acuerdo con la reivindicación 12, caracterizado porque la transmisión de datos entre un sistema de acceso (3.1, 3.2, 3.n) de un contenedor de basura (2.1, 2.2, 2.n) y el sistema de gestión de datos (1) se lleva a cabo en forma inalámbrica.
- 10 14. Procedimiento de acuerdo con la reivindicación 12 o 13, caracterizado porque la transmisión de datos entre un sistema de acceso (3.1, 3.2, 3.n) de un contenedor de basura (2.1, 2.2, 2.n) y el sistema de gestión de datos (1) se realiza mediante una conexión celular, que se selecciona preferiblemente de un grupo formado por una conexión GSM, una conexión UMTS, una conexión GPRS y una conexión LTE.
- 15 15. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8 a 14, caracterizado porque los pasos b, e, f y g se realizan repitiéndolos en forma periódica, teniendo lugar la repetición preferiblemente en un intervalo que se selecciona de un grupo que comprende la repetición diaria, semanal, mensual, trimestral, semestral o anual.

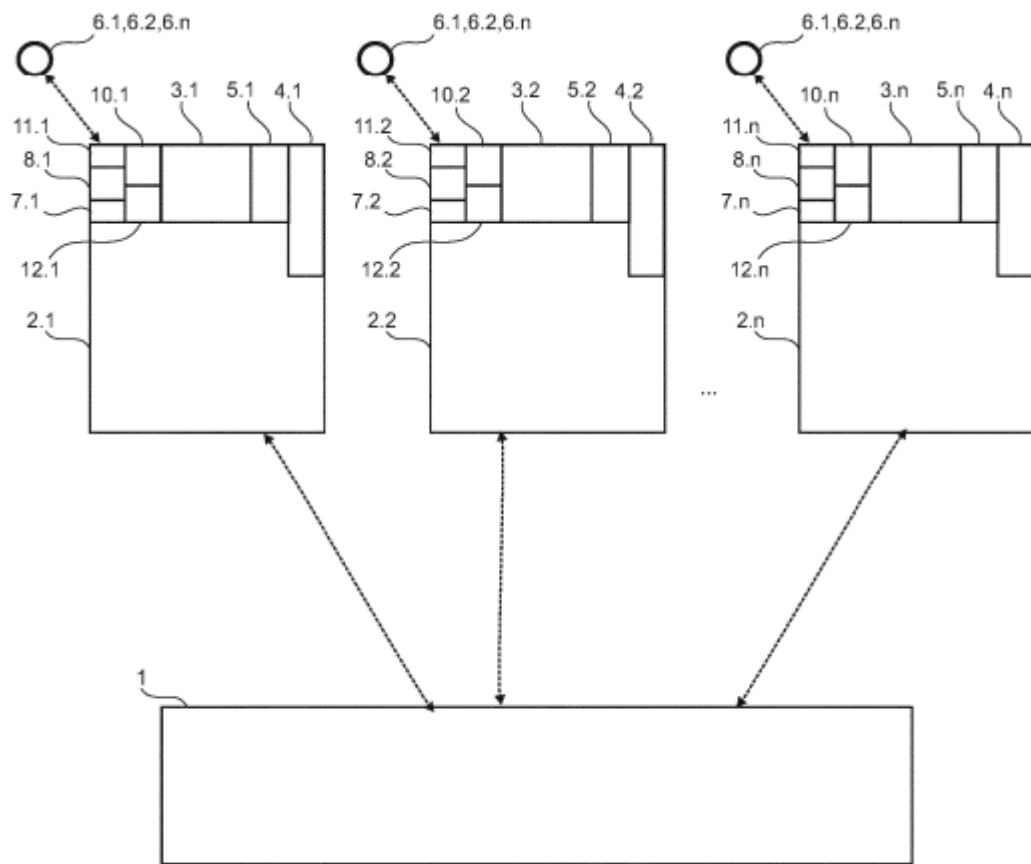


Fig. 1

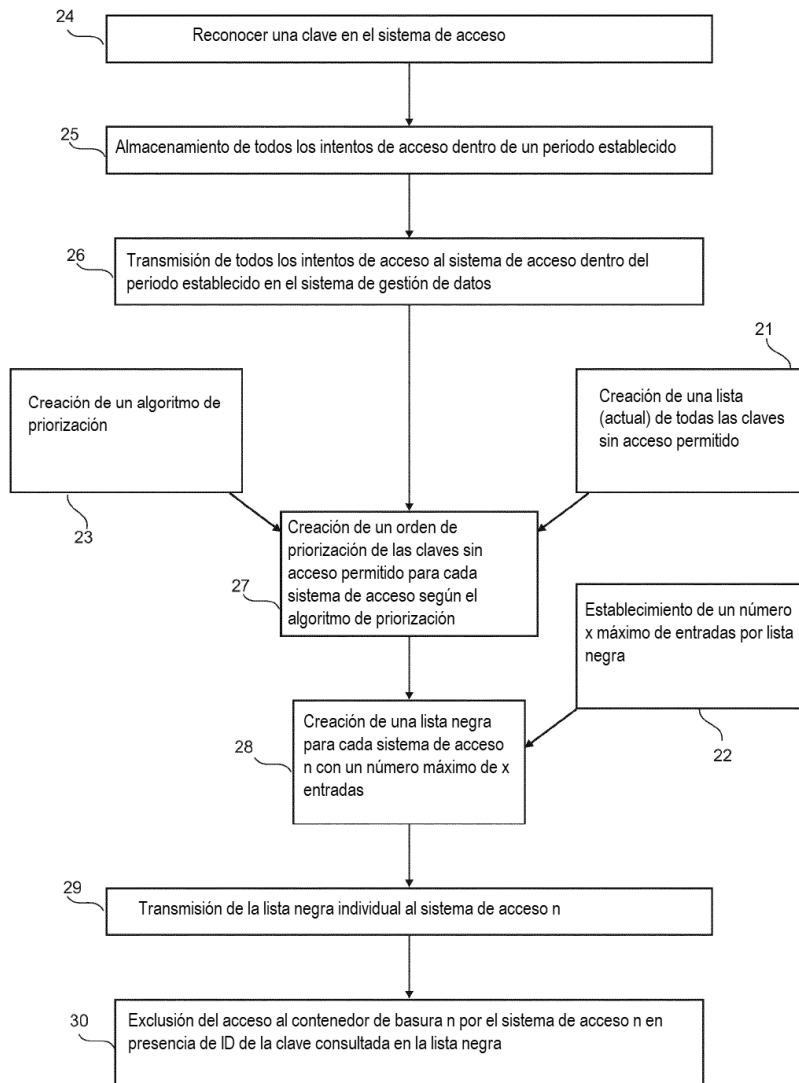


Fig. 2

