



(11)

EP 3 483 841 B1

(12)

EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des
Hinweises auf die Patenterteilung:
04.08.2021 Patentblatt 2021/31

(51) Int Cl.:
G07C 9/00 (2020.01)

(21) Anmeldenummer: **17201190.0**

(22) Anmeldetag: **10.11.2017**

(54) **ELEKTRONISCHES SPERRLISTENVERWALTUNGSSYSTEM UND VERFAHREN ZUR
BERECHTIGUNGSKONTROLLE ZUR BENUTZUNG EINES MÜLLAUFNAHMEBEHÄLTNISSES**

ELECTRONIC BLOCKING LIST MANAGEMENT SYSTEM AND RIGHTS CONTROL METHOD FOR
USING A REFUSE CONTAINER

SYSTÈME DE GESTION DE LISTE NOIRE ÉLECTRONIQUE ET PROCÉDÉ D'HABILITATION DE
L'UTILISATION D'UN RÉCIPIENT À DÉCHETS

(84) Benannte Vertragsstaaten:
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

(43) Veröffentlichungstag der Anmeldung:
15.05.2019 Patentblatt 2019/20

(73) Patentinhaber: **emz-Hanauer GmbH & Co. KGaA
92507 Nabburg (DE)**

(72) Erfinder: **Altenhofer, Herbert
93183 Kallmünz (DE)**

(74) Vertreter: **Hannke, Christian
Hannke Bittner & Partner
Patent- und Rechtsanwälte mbB
Prüfeninger Straße 1
93049 Regensburg (DE)**

(56) Entgegenhaltungen:
KR-A- 20150 051 931 US-A1- 2015 307 273

EP 3 483 841 B1

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

Beschreibung

[0001] Die Erfindung betrifft ein elektronisches Sperrlistenverwaltungssystem und ein Verfahren zur Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses. Das Verfahren zeichnet sich dadurch aus, dass es innerhalb einer Ausschlussliste Einträge gemäß der Wahrscheinlichkeit für einen Anmeldeversuch priorisiert werden, umso schneller und mit verringertem Datenverarbeitungsaufwand die Benutzung eines Müllaufnahmebehältnisses durch nicht autorisierte Nutzer zu unterbinden.

[0002] Zur Entsorgung von Hausmüll werden oft großräumige Müllcontainer bereitgestellt, welche von mehreren Haushalten benutzt werden. Derartige Müllcontainer können beispielsweise einer Hausgemeinschaft oder auch einer Kommune zugehörig sein. In der Regel sollen nur registrierte Benutzer einen Zugang zu solchen Müllcontainern erhalten, wobei der Zugang gesperrt werden kann beispielsweise bei Nichtzahlung der Entsorgungskosten. Ein solcher Zugang kann mittels verschiedenster elektronischer Systeme realisiert werden. Aus dem Stand der Technik ist beispielsweise bekannt, dass einem Benutzer ein Identifikationscode zugewiesen wird. Dieser Identifikationscode ist beispielsweise auf einem Chip oder einer Karte gespeichert, welche der Benutzer in oder an (z.B. bei Nutzung von Funkübertragungstechnik des Identifikationscodes (z.B. mittels RFID)) ein kompatibles Lesegerät führt, um sich zu identifizieren. Der entsprechende Authentifizierungsprozess wird entweder durch eine lokale Steuereinheit in dem Müllcontainer oder über einen zentralen Server, welcher mit der lokalen Steuereinheit des Müllcontainers in Verbindung steht, vorgenommen. Nach der erfolgreichen Authentifizierung und der Zuordnung des Identifikationscodes zu der zugriffsberechtigten Gruppe wird der Müllcontainer dann temporär geöffnet und der Benutzer kann seinen Müll entsorgen.

[0003] Bei elektronischen Zugangssystemen, bei denen (beschreibbare) Schlüssel mit eindeutiger ID verwendet werden (z.B. Transponder mit RFID-Chips), kann es notwendig werden, einzelne oder mehrere dieser Schlüssel zu sperren. Die Notwendigkeit besteht beispielsweise dann, wenn ein Schlüssel verloren geht und verhindert werden muss, dass dieser durch Unberechtigte weiterhin am Zugangssystem verwendet wird. Während es für elektronische Zugangssysteme, zu denen nur wenige Teilnehmer Zugang erhalten sollen (wie z.B. einer Restmülltonne für ein Ein- oder Zweifamilienhaus), vorteilhaft ist, nur diesen Bewohnerkreis mittels einer Liste von zugelassenen Identifikationscodes ("Whitelist") als Zugangsberechtigte zu identifizieren, würde die Verwaltung von Listen mit sehr vielen Einträgen von zugelassenen Identifikationscodes beispielsweise für zentrale Altglas-, Altkleider- oder Grünschnittcontainern, zu denen beispielsweise alle Bewohner einer Stadt Zugang haben, einen hohen Datenverarbeitungsaufwand bedeuten. Stehen einem Zugangssystem sehr viele

Schlüssel gegenüber, können sehr viele Identifikationscodes erforderlich werden, die in jedem Zugangssystem hinterlegt werden müssen. Dies hat mehrere Nachteile, insbesondere a) ist ein großer Speicherbedarf für die Identifikationscodes erforderlich, b) fällt ein hohes Datenvolumen bei der Übertragung der großen Identifikationscodeslisten an, c) sind häufige Aktualisierungen der Identifikationscodeslisten aller Zugangssysteme eines Gebiets notwendig und d) können sich bei großen Identifikationscodeslisten lange Suchzeiten ergeben, durch welche für die Benutzer längere durch die Identifizierung hervorgerufene Wartezeiten entstehen, bevor eine eventuelle Zugangsberechtigung erteilt wird. Für derartige Systeme bietet es sich daher an, die Liste von zugangsberechtigten Identifikationscodes durch eine vergleichsweise kurze Liste von Identifikationscodes zu ersetzen, für die der Zugang zum Entsorgungssystem ausgeschlossen ist ("Blacklist").

[0004] Für eine solche Blacklist muss im Speicherbereich des Zugangssystems eine Liste mit den Sperreinträgen (gesperrte Identifikationscodes) hinterlegt werden, die bei der Authentifizierung eines Schlüssels durchsucht wird. In einigen der oben genannten Fälle, bei denen beispielsweise nahezu alle Bewohner einer Stadt Zugang zum Entsorgungssystem haben, können jedoch aus unterschiedlichen Gründen auch diese Blacklists in kurzer Zeit sehr lang werden, so dass auch hier die oben bezüglich der Whitelist entstehenden Nachteile auftreten können.

[0005] Einem solchen Zugangssystem müssen beispielsweise durch Wegzug von Bewohnern, Nichtzahlung von Gebühren oder Verlust von Schlüsseln oder Karten, ebenfalls in kurzer Zeit viele gesperrte Identifikationscodes mitgeteilt und in der Blacklist hinterlegt werden. Daraus resultiert auch in diesem Fall, dass a) ein großer Speicherbedarf für die Sperreinträge erforderlich wäre, b) ein hohes Datenvolumen bei der Übertragung der großen Sperrlisten anfällt, c) häufige Aktualisierungen der Sperrlisten aller Zugangssysteme eines Gebiets notwendig sind und d) sich bei großen Sperrlisten lange Suchzeiten ergeben können. Die Generierung der Sperrlisten (Blacklists) für Zugangssysteme erfolgt in der Regel durch den örtlichen Entsorgungsdienstleister mittels eines geeigneten Datenmanagementsystems. Die KR20150051931 A offenbart ein System von Müllaufnahmebehältnissen, bei denen im Zuge der Zugangskontrollen eine Sperrliste verwendet wird, welche von einem Sperrlistenmanagementserver verwaltet wird, wobei der Server von einem Müllaufnahmebehältnis erhaltene Sperrlisteninformationen an die anderen Müllaufnahmebehälter, deren Sperrliste diese Informationen noch nicht enthält, weiterleitet.

[0006] Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein System und ein Verfahren zur Datenverwaltung zur Verfügung zu stellen, welches eine effektive und insbesondere schnellere Verarbeitung einer Sperrliste für eine elektronische Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses

ermöglicht.

[0007] Diese Aufgabe wird gelöst durch ein elektronisches Sperrlistenverwaltungssystem für eine Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses gemäß Patentanspruch 1 sowie durch ein Verfahren zur Datenverwaltung einer Sperrliste in einem Zugangssystem für eine elektronische Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses gemäß Patentanspruch 8.

[0008] Vorrichtungsseitig ist somit vorgesehen, dass das elektronische Sperrlistenverwaltungssystem für eine Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses ein Datenmanagementsystem und eine Vielzahl von Zugangssystemen für eine elektronische Berechtigungskontrolle zur Benutzung eines jedem einzelnen Zugangssystem zugeordneten einzelnen Müllaufnahmebehältnisses umfasst. Die Zugangssysteme sind mittels einer Vielzahl von Schlüsseln, die jeweils einem Benutzer oder einer Benutzergruppe zuordenbar sind, aktivierbar. Sowohl das Datenmanagementsystem als auch jedes der Zugangssysteme weist eine Kommunikationsschnittstelle auf, mittels der Daten zwischen dem Datenmanagementsystem und jedem einzelnen Zugangssystem austauschbar sind. Weiterhin weist jedes Zugangssystem eine Speichereinrichtung zum Erstellen und Speichern einer Liste der in einem festgelegten Zeitraum an diesem Zugangssystem verwendeten Schlüssel sowie Mittel zur Übertragung dieser Liste mittels der Kommunikationsschnittstelle an das Datenmanagementsystem auf. Bevorzugt weist ein solches Zugangssystem auch eine Zeiterfassungseinrichtung auf, so dass jedem Zugangsversuch mittels eines Schlüssels ein Zeitstempel zugefügt werden kann. Bevorzugt wird der Zeitstempel mit dem jeweiligen Eintrag des Zugangsversuchs des an diesem Zugangssystem verwendeten Schlüssels abgespeichert. Insbesondere ist bevorzugt, dass der Zeitstempel zusammen mit dem jeweiligen Eintrag des Zugangsversuchs des an diesem Zugangssystem verwendeten Schlüssels an das Datenmanagementsystem übertragen wird. Dadurch kann das Datenmanagementsystem, welches bevorzugt eine größere Speicherkapazität aufweist und über eine größere Rechenleistung als das Zugangssystem verfügt, die Daten über Zugangsversuche mit bestimmten Schlüsseln zusammen mit dem Zeitstempel archivieren. Somit wird die Nutzbarkeit der vom Zugangssystem ermittelten Daten über Zugangsversuche über einen langen Zeitraum gewährleistet.

[0009] Das Datenmanagementsystem weist Einrichtungen zum Erstellen einer Sperrliste für das Zugangssystem eines Müllaufnahmebehältnisses auf, wobei das Datenmanagementsystem dazu eingerichtet ist, beim Erstellen der Sperrliste auf einen Priorisierungsalgorithmus zur Priorisierung von Einträgen in der Sperrliste zurückzugreifen. Der Priorisierungsalgorithmus berücksichtigt dabei zumindest auch das Merkmal der letzten Nutzung eines nicht zugangsberechtigten Schlüssels an dem Zugangssystem des jeweiligen Müllaufnahmebe-

hältnisses. Durch die Nutzung des Merkmals der letzten Nutzung eines nicht zugangsberechtigten Schlüssels an dem Zugangssystem des jeweiligen Müllaufnahmebehältnisses kann verhindert werden, dass Schlüssel, die zerstört oder verloren und nicht wiedergefunden wurden, nicht mehr auf der Sperrliste geführt werden müssen und somit keinen Speicherplatz blockieren. Falls ein verlorener Schlüssel wiedergefunden würde, wäre er - falls er aufgrund der langen Nichtbenutzung nicht mehr auf der Sperrliste enthalten wäre - so zwar wieder nutzbar, da er nicht auf der Sperrliste ist, jedoch würde er bei der nächsten Aktualisierung aufgrund der erneuten Nutzung der Sperrliste wieder zugefügt werden und aufgrund der kürzlichen Nutzung mit entsprechend hoher Priorität in der Sperrliste gelistet.

[0010] Jedes Zugangssystem weist darüber hinaus eine Speichereinrichtung zum Speichern der vom Datenmanagementsystem und von diesem an das jeweilige Zugangssystem übertragenen Sperrliste für das diesem Zugangssystem zugeordneten Müllaufnahmebehältnisses auf. Dadurch steht die Sperrliste diesem Zugangssystem auch nach der Datenübertragung für den Abgleich mit Schlüsseln zur Verfügung, die die Nutzung des zugeordneten Müllaufnahmebehältnisses anfragen. Eine bestehende Datenverbindung zum Datenmanagementsystem ist somit nicht notwendig. Außerdem umfasst jedes Zugangssystem eine Datenverarbeitungseinrichtung und eine Steuerungseinrichtung zum Gewähren oder Verweigern des Zugangs zu dem dem Zugangssystem zugeordneten Müllaufnahmebehältnis für einen dem Schlüssel zugeordneten Benutzer, wobei eine Zugangsverweigerung eine Folge eines erfolgreichem Abgleich des Schlüssels mit den in der Sperrliste enthaltenden Einträgen ist. Die Datenverarbeitungseinrichtung vergleicht einen die Benutzung des dem Zugangssystem zugeordneten Müllaufnahmebehältnisses anfragenden Schlüssel mit den in der Sperrliste enthaltenden Einträgen. Sofern der Schlüssel nicht von der Benutzung des dem Zugangssystem zugeordneten Müllaufnahmebehältnisses ausgeschlossen ist, kann durch die Steuerungseinrichtung der Zugang zu dem Müllaufnahmebehältnis gewährt werden.

[0011] Bevorzugt ist jedem Zugangssystem genau ein Müllaufnahmebehältnis zugeordnet. Somit kann ein Zugangssystem den Zugang zu dem diesem zugeordneten Müllaufnahmebehältnis kontrollieren.

[0012] Die Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses erfolgt mittels Schlüsseln. Einem Benutzer oder einer Benutzergruppe ist jeweils ein Schlüssel zugeordnet. Bei einem solchen Schlüssel kann es sich beispielsweise um eine Identifikationsnummer (ID) handeln. Diesbezüglich sei angemerkt, dass der Begriff Identifikationsnummer nicht auf Nummern beschränkt ist, sondern allgemein für jegliche Zeichenfolge verwendet wird, die eine Zuordnung zu einem Benutzer ermöglicht. Diese ID kann beispielsweise ein von dem Benutzer einzugebender PIN (Persönliche Identifikationsnummer (PIN-Code)) sein oder auf einem

von dem Zugangssystem lesbaren Datenträger gespeichert sein. Bei einem solchen lesbaren Datenträger handelt es sich bevorzugt um einen Datenträger, der ausgewählt ist aus einer Gruppe, die eine Chipkarte, einen RFID-Tag, ein Mobiltelefon, ein Tablet, einen Laptop, einen Finger (Fingerabdruck), das Gesicht (Gesichtsscan) und ein Auge (Irisscan) umfasst. Aufgrund des geringeren apparativen Aufwands und des geringeren Energieverbrauchs sind insbesondere eine Chipkarte, ein RFID-Tag oder ein Mobiltelefon (z.B. über NFC (Nahfeldkommunikation (Near Field Communication) oder Bluetooth) zur Identifikation eines Benutzers bevorzugt. Die NFC-Technologie ist besonders bevorzugt, da mittlerweile nahezu alle Smartphones diese Technologie unterstützen und somit eine sehr weite Verbreitung von entsprechenden Identifikationsgeräten besteht.

[0013] Üblicherweise benötigt ein Zugangssystem für die Kontrolle und Steuerung des Zugangs zu dem Müllaufnahmebehältnis Energie, in der Regel elektrischen Strom. Da sich die Müllaufnahmebehältnisse oftmals im öffentlichen Raum befinden, ist in vielen Fällen kein Zugang zu einem Stromnetz vorhanden. Daher ist eine dezentrale Energieversorgung bevorzugt. Diese könnte beispielsweise durch Batterien, Akkumulatoren oder Solarstrom erfolgen. Auch Kombinationen dieser oder Ergänzungen mit anderen Energiequellen sind möglich. Beispielsweise ist denkbar, dass die benötigte Energie durch Solarenergie gewonnen und in Akkumulatoren gespeichert wird. Eine Batterie als Notstromquelle, falls keine anderen Energiequellen zur Verfügung stehen, wäre ebenfalls (unabhängig und in Kombination mit anderen Energiequellen) denkbar.

[0014] Da wie oben erwähnt bei derartigen Systemen ein Zugang zum Stromnetz oftmals nicht vorhanden ist, ist bei der Steuerung und Überwachung des Zugangs zu dem Müllaufnahmebehältnis die Verwendung von energieintensiven Datenverarbeitungssystemen nur sehr eingeschränkt möglich. Die damit verbundenen Grenzen in der Leistungsfähigkeit der Datenverarbeitungssysteme führen zu der eingangs erwähnten Verzögerung bei der Überprüfung von Zugangsberechtigungen aus einer Liste mit sehr vielen Einträgen. Um derartige Verzögerungen zu vermeiden oder zumindest zu reduzieren ist es erforderlich, eine maximale Anzahl von Einträgen in eine Liste festzulegen, aus der die Zugangsberechtigung ermittelt wird. Insbesondere bei Systemen mit sehr vielen Zugangsberechtigten scheidet daher (wie eingangs beschrieben) eine Whitelist aus. Systemen mit sehr vielen Zugangsberechtigten lassen sich besonders effizient mittels einer Blacklist oder Sperrlisteneinträgen verwalten. Da auch Listen mit Sperrlisteneinträgen mit der Zeit eine kritische Größe überschreiten können, ist auch hierfür eine maximale Anzahl der Sperrlisteneinträge festzulegen, um deren schnelle Verarbeitung durch das Zugangssystem gewährleisten zu können.

[0015] Bevorzugt ist vorgesehen, dass ein Zugangssystem eine Schleuseneinrichtung mit einer Verriegelungseinrichtung aufweist. Die Schleuseneinrichtung

kann beispielsweise dazu genutzt werden, Müll in das Müllaufnahmebehältnis einzuwerfen. Nur wenn eine Verriegelungseinrichtung entriegelt ist, kann ein Schleusenzugang durch den Benutzer (oder auch das Zugangssystem selbst) geöffnet werden. In einer bevorzugten Ausführungsform gibt die Steuerungseinrichtung ein Freigabesignal zum Entriegeln der Verriegelungseinrichtung ab. Dies erfolgt jedoch nur, wenn der Abgleich des Schlüssels mit den in der Sperrliste enthaltenden Einträgen in der Datenverarbeitungseinrichtung negativ ist.

[0016] Aufgrund der oftmaligen Anordnung der Müllaufnahmebehältnisse im frei zugänglichen öffentlichen Raum ist oftmals auch der Zugang zu einem kabelgebundenen Datennetz nicht vorhanden oder sehr eingeschränkt. Daher ist in einer bevorzugten Ausführungsform die Kommunikationsschnittstelle zum Austausch der Daten zwischen dem Datenmanagementsystem und jedem einzelnen Zugangssystem eine zur drahtlosen Kommunikation geeignete Kommunikationsschnittstelle. Aufgrund der großen Netzabdeckung ist hierbei insbesondere eine Mobilfunkkommunikationseinrichtung bevorzugt, welche insbesondere bevorzugt ausgewählt ist aus einer Gruppe, die eine GSM-, eine UMTS-, eine GPRS- und eine LTE-Mobilfunkkommunikationseinrichtung umfasst. Alternativ oder ergänzend dazu wäre auch eine WLAN-Verbindung (Verbindung über ein drahtloses lokales Netzwerk (Wireless Local Area Network)) denkbar, da in vielen Städten mittlerweile auch ein solches Netzwerk zur Verfügung steht. Alternativ zu der drahtlosen Datenübertragung wäre auch die Übertragung mittels eines Datenträgers (beispielsweise einer Speicherkarte oder eines Speicherstifts (z.B. USB-Stick) möglich. Dies könnte beispielsweise bei oder während der Leerung des Müllaufnahmebehältnisses erfolgen. Da oftmals die Datenübertragung nicht zeitkritisch ist und beispielsweise über Nacht oder während Zeiten geringer Nutzung des Übertragungsnetzes erfolgen kann, ist die Geschwindigkeit der Datenübertragung insbesondere bei einer drahtlosen Datenübertragung von untergeordneter Bedeutung.

[0017] In einer weiteren bevorzugten Ausführungsform weist ein Zugangssystem und/oder ein Müllaufnahmebehältnis eine Lokalisierungseinrichtung auf, durch welche der aktuelle Standort des Müllaufnahmebehältnisses ermittelbar ist. Weiter bevorzugt nutzt die Lokalisierungseinrichtung zur Bestimmung des aktuellen Standorts ein globales Navigationssatellitensystem. Insbesondere bevorzugt ist dieses ausgewählt aus einer Gruppe, die NAVSTAR GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo und Beidou umfasst. Der aktuelle Standort ist bevorzugt an das Datenmanagementsystem übertragbar, bevorzugt über die oben bereits erwähnte Kommunikationsschnittstelle. Die Ermittlung und die Übertragung des aktuellen Standorts des Müllaufnahmebehältnisses an das Datenmanagementsystem hat den Vorteil, dass ein z.B. durch Vandalismus oder Diebstahl vom vorgesehenen Standort entferntes Müllaufnahmebehältnis

leicht lokalisierbar ist. Darüber hinaus können auch die in der Umgebung dieses Müllaufnahmebehältnisses befindlichen weiteren Müllaufnahmebehältnisse ermittelt werden, was wie später dargestellt, für die Ermittlung der Sperrlisten Berücksichtigung finden kann.

[0018] Von besonderer Bedeutung für eine effiziente Zuordnung einzelner Schlüssel zu den Sperrlisten einzelner Müllaufnahmebehältnisse bzw. dem jeweiligen, diesem Müllaufnahmebehältnis zugeordneten Zugangssystem ist der Priorisierungsalgorithmus. Bevorzugt ist durch die Nutzung dieses Priorisierungsalgorithmus eine Sperrliste generierbar, die einerseits möglichst kurz ist, andererseits jedoch so viele Sperreinträge enthält, dass eine unberechtigte Nutzung des jeweiligen Müllaufnahmebehältnisses mit hoher Wahrscheinlichkeit verhindert oder zumindest minimiert wird.

[0019] In einer bevorzugten Ausführungsform umfasst der Priorisierungsalgorithmus Rechenvorschriften, die mindestens ein Merkmal abbilden, das ausgewählt ist aus einer Gruppe, die

- die Häufigkeit der Nutzung eines nicht zugangsberechtigten Schlüssels an dem Zugangssystem des jeweiligen Müllaufnahmebehältnisses,
- die letzte Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem eines anderen Müllaufnahmebehältnisses, welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnis angeordnet ist,
- die Häufigkeit der letzten Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem eines anderen Müllaufnahmebehältnisses, welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnis angeordnet ist,
- die Höhe eines ausstehenden Rechnungsbetrags des diesem Schlüssel zugeordneten Benutzers und
- die geographische Verteilung der Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem anderer Müllaufnahmebehältnisse

[0020] Durch die Abbildung einer oder mehrerer dieser Merkmale in den Rechenvorschriften des Priorisierungsalgorithmus können verschiedene denkbare Szenarien der missbräuchlichen Nutzung eines Schlüssels vorhergesehen und die entsprechenden Zugangssysteme der jeweiligen Müllaufnahmebehältnisse auf die wahrscheinlich eintretende missbräuchlichen Nutzung eines Schlüssels durch dessen Aufnahme in die jeweilige Sperrliste vorbereitet werden.

[0021] Ist beispielsweise die Häufigkeit der Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem eines bestimmten Müllaufnahmebehältnisses sehr hoch, ist mit großer Wahrscheinlichkeit zu erwarten, dass der (nun) nicht mehr zur Nutzung zugelassene Benutzer dennoch mit hoher Wahrscheinlichkeit wieder dieses Müllaufnahmebehältnis nutzen möchte. Durch eine entsprechend hohe Priorisierung dessen

Schlüssels an der individuell für dieses Müllaufnahmebehältnis erstellten Sperrliste, kann der missbräuchlichen Nutzung vorgebeugt werden.

[0022] Ebenso ist die Wahrscheinlichkeit hoch, dass ein nicht (mehr) zugangsberechtigter Nutzer versuchen wird, Müllaufnahmebehältnisse in der Nähe des zuvor bevorzugten und meist genutzten Müllaufnahmebehältnisses zu nutzen. Da (wie oben erwähnt) die (aktuelle) Position der einzelnen Müllaufnahmebehältnisse bekannt, überwacht oder bei Bedarf ermittelt werden kann, können so schnell Müllaufnahmebehältnisse ermittelt werden, welche geographisch in einem vordefinierten Abstand vom zuletzt durch den auszuschließenden Nutzer genutzten Müllaufnahmebehältnis angeordnet sind. Lag die letzte Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem eines anderen Müllaufnahmebehältnisses, welches geographisch in einem vordefinierten (geringen) Abstand vom jeweiligen Müllaufnahmebehältnis angeordnet ist nicht lange zurück, kann dies für eine hohe Priorisierung dieses Schlüssels auch an einem zuvor noch nicht von diesem Nutzer verwendeten Müllaufnahmebehältnis genutzt werden.

[0023] Ist die Häufigkeit der letzten Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem eines anderen Müllaufnahmebehältnisses, welches geographisch in einem vordefinierten (geringen) Abstand vom jeweiligen Müllaufnahmebehältnis angeordnet ist sehr hoch, kann dies ebenfalls darauf hinweisen, dass der unberechtigte Nutzer in diesem Gebiet häufig aktiv ist und mit hoher Wahrscheinlichkeit in Zukunft auch dieses Müllaufnahmebehältnis nutzen könnte. Eine hohe Priorisierung dieses Schlüssels auch an diesem Müllaufnahmebehältnis führt auch vor dem ersten Benutzungsversuch bereits zu einer Verweigerung der Nutzung.

[0024] Ebenso wäre es denkbar die geographische Verteilung der Nutzung eines (nun) nicht (mehr) zugangsberechtigten Schlüssels an einem Zugangssystem anderer Müllaufnahmebehältnisse der Priorisierung zugrunde zu legen. Nutzte ein Benutzer beispielsweise bisher vorwiegend zwei verschiedene Müllaufnahmebehältnisse (z.B. am Wohnort und an der Arbeitsstätte) könnten durch die Berücksichtigung der geographischen Verteilung der Nutzung dieser Müllaufnahmebehältnisse auch geographisch dazwischenliegende (z.B. im Bereich der Hauptverkehrsstraßen) Müllaufnahmebehältnisse von der Nutzung für diesen Benutzer ausgeschlossen werden, indem dieser mit entsprechend hoher Priorisierung in den jeweiligen Sperrlisten der Zugangssysteme der dort positionierten Müllaufnahmebehältnisse aufgenommen wird.

[0025] Ein weiteres mögliches Kriterium für eine hohe Priorisierung könnte die Höhe eines ausstehenden Rechnungsbetrags des diesem Schlüssel zugeordneten Benutzers sein. Durch eine solche hohe Priorisierung kann Nutzern, die über einen langen Zeitraum Rechnungen nicht bezahlen auch die Nutzung von Müllaufnahmebehältnissen untersagt werden, die sehr weit von den

üblicherweise genutzten Müllaufnahmebehältnissen entfernt liegen und auf deren Sperrliste aufgrund der großen Entfernung dieser säumige Nutzer aufgrund der oben dargestellten Kriterien sonst nicht geführt würde.

[0026] In einer bevorzugten Ausführungsform zeichnet sich das elektronisches Sperrlistenverwaltungssystem dadurch gekennzeichnet, dass zumindest eines der Zugangssysteme, bevorzugt eine Vielzahl von Zugangssystemen, weiter bevorzugt alle Zugangssysteme, eine Einrichtung zum Ausschluss eines Schlüssels zu allen Zugangssystemen des elektronischen Sperrlistenverwaltungssystem aufweist. Eine solche Einrichtung zum Ausschluss eines Schlüssels zu allen Zugangssystemen des elektronischen Sperrlistenverwaltungssystems könnte in einer bevorzugten Ausführungsform beispielsweise eine Vorrichtung zum Einziehen des Schlüssels oder zum Löschen, Überschreiben oder anderwärtig Unbrauchbarmachen einer auf dem Schlüssel gespeicherten Identifikationsnummer sein.

[0027] Werden beispielsweise zur Identifizierung Chipkarten verwendet, könnten diese durch das Zugangssystem nach (evtl. mehrmaligen) unberechtigten bzw. abgelehnten Zugangsversuchen einbehalten werden. Bei einer Leerung des Müllaufnahmebehältnisses könnte durch das Bedienpersonal auch die einbehaltene Chipkarte aus dem Zugangssystem entnommen werden und so aus dem Verkehr gezogen werden.

[0028] Bei einer Identifikation über einen Schlüssel, der nicht physisch in Kontakt mit dem Zugangssystem gebracht werden muss (z.B. einem RFID-Tag, einem Mobiltelefon oder einem anderen kontaktlos arbeitenden System), ist das Einbehalten meist nicht möglich, so dass der Schlüssel durch Löschen, Überschreiben oder auf anderwärtige andere Weise unbrauchbar gemacht werden könnte. Denkbar wäre beispielsweise, dass alle Schlüssel eines Gebietes einen einheitlichen Präfix enthalten, welcher sie als diesem Gebiet (z.B. einer Stadt, einem Stadtteil, einem Ort oder einem Landkreis) zugehörig klassifiziert. Wird dieses Präfix gelöscht, überschrieben oder auf andere Weise unbrauchbar gemacht, reagieren die Zugangssysteme dieses Gebiets nicht mehr auf diesen Schlüssel, so dass die Nutzung dieses Schlüssels für das gesamte Gebiet ausgeschlossen wird.

[0029] Erkennt ein Zugangssystem während des Authentifizierungsvorgangs die ID eines unberechtigten Schlüssels, kann somit das Zugangssystem die Daten des unberechtigten Schlüssels durch einen Schreibzugriff gezielt zerstören oder zumindest derart verändern, dass dessen Funktion gestört ist. Somit funktioniert der Authentifizierungsvorgang des unberechtigten Schlüssels auch an keinem anderen Zugangssystem mehr.

[0030] Besonders bevorzugt ist in diesem Zusammenhang, wenn die Information eines zerstörten Schlüssels von dem zerstörenden Zugangssystem an das Datenmanagementsystem übertragen wird. Dadurch kann der Sperreintrag dieses Schlüssels aus allen Sperrlisten gelöscht werden, wodurch ein freier Platz für einen weiteren

unberechtigten Schlüssel geschaffen werden kann.

[0031] Verfahrensseitig wird die der Erfindung zugrundeliegende Aufgabe durch ein Verfahren zur Datenverwaltung einer Sperrliste in einem Zugangssystem für eine elektronische Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses gelöst, mit den Schritten

- a. Festlegen einer maximalen Anzahl der Sperrlisteneinträge,
- b. Übertragung der in einem festgelegten Zeitraum an dem Zugangssystem jedes einzelnen Müllaufnahmebehältnisses aus einer Vielzahl von Müllaufnahmebehältnissen bisher verwendeten Schlüssel an ein Datenmanagementsystem,
- c. Sofern die maximale Anzahl der Sperrlisteneinträge noch nicht erreicht ist: Aufnahme der nicht zugangsberechtigten Schlüssel in die Sperrliste und Übertragung der Sperrliste an die Zugangssysteme aller Müllaufnahmebehältnisse durch das Datenmanagementsystem, oder falls die maximale Anzahl der Sperrlisteneinträge erreicht ist:
- d. Festlegen eines Priorisierungsalgorithmus zur Priorisierung von Einträgen in einer Sperrliste für das Zugangssystem eines Müllaufnahmebehältnisses, wobei der Priorisierungsalgorithmus zumindest auch das Merkmal der letzten Nutzung eines nicht zugangsberechtigten Schlüssels an dem Zugangssystem des jeweiligen Müllaufnahmebehältnisses berücksichtigt,
- e. Erstellen jeweils einer individuellen Priorisierungsrangfolge aller nicht zugangsberechtigten Schlüssel für das Zugangssystem jedes einzelnen definierten Müllaufnahmebehältnisses durch das Datenmanagementsystem,
- f. Aufnahme der nicht zugangsberechtigten Schlüssel beginnend mit dem Schlüssel mit der höchsten Priorisierung in absteigender Rangfolge der Priorisierung in die individuelle Sperrliste des Zugangssystems jedes einzelnen definierten Müllaufnahmebehältnisses bis die maximalen Anzahl der Sperrlisteneinträge erreicht ist durch das Datenmanagementsystem,
- g. Übertragung der individuellen Sperrliste an das Zugangssystem jedes einzelnen definierten Müllaufnahmebehältnisses und
- h. Gewährung oder Verweigerung des Zugangs zu einem definierten Müllaufnahmebehältnis gemäß der in der individuellen Sperrliste des Zugangssystems des jeweiligen definierten Müllaufnahmebehältnisses hinterlegten Schlüssel, auszeichnet.

[0032] Das Festlegen einer maximalen Anzahl der Sperrlisteneinträge erfolgt, wie bereits oben dargestellt, bevorzugt in Abhängigkeit der Leistungsfähigkeit des jeweiligen Zugangssystems. Da eine geringe Anzahl der Sperrlisteneinträge eine vergleichsweise schnelle Datenverarbeitung auch bei vergleichsweise leistungs-

schwachen Zugangssystemen ermöglicht, ist eine geringe maximale Anzahl von Sperrlisteneinträgen bevorzugt. Besonders bevorzugt liegt die maximale Anzahl von Sperrlisteneinträgen bei 5000 Einträgen, weiter bevorzugt bei 2¹² Einträgen, weiter bevorzugt bei 2¹¹ Einträgen, besonders bevorzugt bei 2¹⁰ Einträgen, weiter bevorzugt bei 1000 Einträgen, weiter bevorzugt bei 2⁵ Einträgen, weiter bevorzugt bei 500 Einträgen, besonders bevorzugt bei 400 Einträgen, weiter bevorzugt bei 2⁸ Einträgen, weiter bevorzugt bei 2⁷ Einträgen und besonders bevorzugt bei 100 Einträgen. Bei einer derart geringen Zahl von Einträgen kann bei aktueller Hardware auch bei äußerst geringer Stromaufnahme ein Abgleich mit einer Sperrliste durch das Zugangssystem nahezu ohne für den Benutzer merkbare Verzögerung erfolgen. Das Festlegen einer maximalen Anzahl der Sperrlisteneinträge muss nicht bei jedem erneuten Erstellen einer Sperrliste erneut durchgeführt werden. Daher soll auch das Beibehalten eines zuvor festgelegten Wertes einer maximalen Anzahl der Sperrlisteneinträge als Festlegen einer maximalen Anzahl der Sperrlisteneinträge im Sinn dieser Erfindung verstanden werden.

[0033] Wie oben dargestellt ist es für die Bewertung der Wahrscheinlichkeit einer missbräuchlichen Nutzung eines Müllaufnahmebehältnisses die letzte (und/oder häufige) Nutzung eines Schlüssels an diesem oder einem geographisch nahegelegenen Müllaufnahmebehältnis von Bedeutung. Daher ist vorgesehen, dass (bevorzugt regelmäßig wiederkehrend) die bisher in einem festgelegten Zeitraum an dem Zugangssystem jedes einzelnen Müllaufnahmebehältnisses aus einer Vielzahl von Müllaufnahmebehältnissen verwendeten Schlüssel an ein Datenmanagementsystem übertragen werden.

[0034] Sofern die maximale Anzahl der Sperrlisteneinträge noch nicht erreicht ist, können alle nicht zugangsberechtigten Schlüssel in die Sperrliste aufgenommen werden. Diese Sperrliste ist für die Zugangssysteme aller Müllaufnahmebehältnisse gleich, so dass diese durch das Datenmanagementsystem an alle Zugangssysteme übertragen werden kann. Spätestens wenn die maximale Anzahl der Sperrlisteneinträge jedoch erreicht ist, ist jedoch vorgesehen, dass ein Priorisierungsalgorithmus zur Priorisierung von Einträgen in einer Sperrliste für das Zugangssystem eines Müllaufnahmebehältnisses festgelegt wird. Der Priorisierungsalgorithmus berücksichtigt dabei zumindest auch das Merkmal der letzten Nutzung eines nicht zugangsberechtigten Schlüssels an dem Zugangssystem des jeweiligen Müllaufnahmebehältnisses. Da somit jeder Zugangsversuch an einzelnen Müllaufnahmebehältnissen zur Erstellung der Sperrlisten berücksichtigt wird, werden individuelle Sperrlisten notwendig. Jedem Müllaufnahmebehältnis wird somit eine individuelle Sperrliste zugeordnet, die zumindest in guter Näherung die Wahrscheinlichkeit für eine missbräuchliche Nutzung eines Schlüssels an genau diesem Müllaufnahmebehältnis widerspiegelt.

[0035] Es wird somit eine individuelle Priorisierungsrangfolge aller nicht zugangsberechtigten Schlüssel für

das Zugangssystem jedes einzelnen definierten Müllaufnahmebehältnisses durch das Datenmanagementsystem erstellt. Basierend auf dieser Priorisierungsrangfolge wird nun beginnend mit dem Schlüssel mit der höchsten Priorisierung in absteigender Rangfolge der Priorisierung eine individuelle Sperrliste für das Zugangssystem jedes einzelnen definierten Müllaufnahmebehältnisses generiert, wobei jeder Eintrag in die individuelle Sperrliste übernommen wird, bis die maximale Anzahl der Sperrlisteneinträge erreicht ist. Alternativ könnte, wenn die Anzahl der Einträge gemäß der Priorisierungsrangfolge die maximal zulässige Anzahl der Sperrlisteneinträge überschreitet, in dieser Rangfolge der jeweils mit geringster Priorisierung gelistete Eintrag gelöscht werden, bis die Anzahl der Schlüssel dieser individuellen Priorisierungsrangfolge der maximal zulässigen Anzahl der Sperrlisteneinträge entspricht. Schlüssel, deren Nutzung an genau diesem Müllaufnahmebehältnis unwahrscheinlich ist, sind in der diesem Müllaufnahmebehältnis zugeordneten Sperrliste nicht enthalten, sofern deren Platzierung in der Priorisierungsrangfolge die maximale Anzahl der Listeneinträge übersteigt.

[0036] Die so generierten individuellen Sperrlisten für jeweils ein bestimmtes Zugangssystem wird anschließend an das Zugangssystem des jeweiligen Müllaufnahmebehältnisses übertragen. Somit steht die Sperrliste mit den für dieses Müllaufnahmebehältnis am wahrscheinlichsten missbräuchlich genutzten Schlüsseln dem dortigen Zugangssystem in Zukunft auch ohne bestehende Datenverbindung zu Verfügung und ermöglicht die Evaluierung einer Zugangsberechtigung für einen bestimmten Schlüssel.

[0037] Versucht nun ein Benutzer mit einem bestimmten Schlüssel Zugang zum Müllaufnahmebehältnis zu erlangen, kann das Zugangssystem gemäß der in der individuellen Sperrliste für das jeweilige Müllaufnahmebehältnis hinterlegten Schlüssel, den Zugang gewähren oder verweigern. Somit ist es nur Benutzern möglich, dieses Müllaufnahmebehältnis zu nutzen, deren Schlüssel nicht in der im Zugangssystem dieses Müllaufnahmebehältnis hinterlegten individuellen Sperrliste enthalten ist.

[0038] Der Begriff "individuelle Sperrliste" soll im Sinn dieser Erfindung derart verstanden werden, dass für jedes Müllaufnahmebehältnis oder jede Gruppe von Müllaufnahmebehältnissen separat eine Sperrliste ermittelt wird. Jedoch ist es durchaus denkbar, dass die separat ermittelten Sperrlisten auch für verschiedene Müllaufnahmebehältnisse identisch sein können. Auch solche identische Sperrlisten sollen als individuelle Sperrliste im Sinn dieser Erfindung verstanden werden.

[0039] Wie bereits oben vorrichtungsseitig beschrieben, ist es auch verfahrensseitig vorteilhaft, wenn der Priorisierungsalgorithmus weiterhin Merkmale berücksichtigt, die ausgewählt sind aus einer Gruppe, die

- die Häufigkeit der Nutzung eines nicht zugangsberechtigten Schlüssels an dem Zugangssystem des jeweiligen Müllaufnahmebehältnisses,

- die letzte Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem eines anderen Müllaufnahmebehältnisses, welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnisses angeordnet ist,
- die Häufigkeit der letzten Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem eines anderen Müllaufnahmebehältnisses, welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnisses angeordnet ist,
- die Höhe eines ausstehenden Rechnungsbetrags des diesem Schlüssel zugeordneten Benutzers und
- die geographische Verteilung der Nutzung eines nicht zugangsberechtigten Schlüssels an einem Zugangssystem anderer Müllaufnahmebehältnisse umfasst.

[0040] Vorteilhafterweise wird bei der Überschreitung einer festgelegten Anzahl von abgelehnten Zugangsversuchen eines nicht zugangsberechtigten Schlüssels der Schlüssel durch das Zugangssystem von der weiteren Nutzung ausgeschlossen. Dies kann bevorzugt dadurch erfolgen, dass das Zugangssystem den Schlüssel einzieht oder eine auf dem Schlüssel gespeicherte Identifikationsnummer löscht, überschreibt oder anderwärtig unbrauchbar macht.

[0041] Bevorzugt ist weiterhin ein Verfahren, bei dem die Datenverarbeitung durch das Datenmanagementsystem örtlich von dem jeweiligen Müllaufnahmebehältnis getrennt vorgenommen wird. Dies hat den Vorteil, dass die Datenverarbeitung durch das Datenmanagementsystem an zentral für alle Müllaufnahmebehältnisse erfolgen kann. Bevorzugt erfolgt sie an einem Ort, an dem ausreichend Strom für den Betrieb eines leistungsfähigen Datenmanagementsystems und optional auch eines Archivierungssystems zur Verfügung steht. Somit können auch Informationen über unberechtigte Zugangsversuche über einen langen Zeitraum archiviert werden und/oder bei der erneuten Nutzung eines für einen langen Zeitraum nicht mehr benutzten Schlüssels die mit diesem verbundenen Nutzungsdaten wieder zur Anwendung kommen.

[0042] Die Übertragung der Daten kann beispielsweise bei der Leerung des jeweiligen Müllaufnahmebehältnisses erfolgen. Bevorzugt ist jedoch eine alternative Verfahrensvariante, bei der die Übertragung von Daten zwischen einem Zugangssystem eines Müllaufnahmebehältnisses und dem Datenmanagementsystem drahtlos erfolgt. Dies ermöglicht den Datenaustausch auch Zeitpunkten zwischen zwei Leerungen, beispielsweise wenn zeitnah die missbräuchliche Nutzung eines Müllaufnahmebehältnisses zu erwarten ist. Bei der drahtlosen Übertragung von Daten ist das Entsenden eines Mitarbeiters zur Aktualisierung der Sperrliste eines Müllaufnahmebehältnisses nicht erforderlich.

[0043] Besonders bevorzugt ist eine Verfahrensvariante, bei der die Übertragung von Daten zwischen einem

Zugangssystem eines Müllaufnahmebehältnisses und dem Datenmanagementsystem mittels einer Mobilfunkverbindung erfolgt, welche bevorzugt ausgewählt ist aus einer Gruppe, die eine GSM-Verbindung, eine UMTS-Verbindung, eine GPRS-Verbindung und eine LTE-Verbindung umfasst.

[0044] In einer bevorzugten Verfahrensvariante werden die oben genannten Schritte b, e, f und g periodisch wiederholend vorgenommen, wobei die Wiederholung bevorzugt in einem Intervall erfolgt, welches ausgewählt ist aus einer Gruppe, die tägliche, wöchentliche, monatliche, quartalsweise, halbjährliche oder jährliche Wiederholung umfasst. Somit kann ein aktueller Datenstand in den Zugangssystemen aller Müllaufnahmebehältnisse gewährleistet werden. Selbstverständlich wäre es auch denkbar das beschriebene System und Verfahren zur Steuerung des Zugangs für Müllaufnahmebehältnisse verschiedener Müllsorten wie beispielsweise Restmüll-, Papier-, Flaschen-, Metall-, Holz-, Grünschnitt-, Sondermüll-, Medikamentenreste- oder Kunststoffsammler anzuwenden.

[0045] Weitere Vorteile, Ziele und Eigenschaften der vorliegenden Erfindung werden anhand nachfolgender Beschreibung der anliegenden Figuren erläutert. Gleichartige Komponenten können in den verschiedenen Ausführungsformen gleiche Bezugszeichen aufweisen.

[0046] In den Figuren zeigen:

Fig. 1 eine Übersichtsdarstellung eines elektronischen Sperrlistenverwaltungssystems für die Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses;

Fig. 2 eine Prinzipskizze des elektronischen Sperrlistenverwaltungssystems für die Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses nach einer Ausführungsform;

Fig. 3 eine beispielhafte Darstellung für die Erstellung einer Priorisierungsrangfolge und einer daraus resultierenden individuellen Sperrliste.

[0047] Figur 1 zeigt eine Übersichtsdarstellung des elektronischen Sperrlistenverwaltungssystems für die Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses. Dieses System umfasst ein Datenmanagementsystem (1). Dieses kann zentral angeordnet sein und ist bevorzugt räumlich von jedem der Müllaufnahmebehältnisse (2.1, 2.2, 2.n) getrennt. Jedes der Müllaufnahmebehältnisse (2.1, 2.2, 2.n) ist mit einem Zugangssystemen (3.1, 3.2, 3.n) verbunden, welches den Zugang zu dem jeweiligen Müllaufnahmebehältnis (2.1, 2.2, 2.n) steuert. Dazu ist eine Schleuseneinrichtung bzw. Übergabeeinrichtung (4.1, 4.2, 4.n) vorgesehen, welche mittels einer Verriegelungseinrichtung (5.1, 5.2, 5.n) verriegelbar ist. Ist die Schleuseneinrichtung (4.1, 4.2, 4.n) verriegelt, ist der Zugang zu dem jeweiligen Müllaufnahmebehältnis (2.1, 2.2, 2.n) versperrt und kein Ein-

wurf von Müll in dieses Müllaufnahmebehältnis (2.1, 2.2, 2.n) möglich.

[0048] Ob einem Benutzer der Einwurf von Müll gestattet wird und die Schleuseneinrichtung (4.1, 4.2, 4.n) durch Entriegeln der Verriegelungseinrichtung (5.1, 5.2, 5.n) durch den Benutzer geöffnet werden kann, wird durch das Zugangssystem (3.1, 3.2, 3.n) anhand eines dem Benutzer zugeordneten Schlüssel, beispielsweise einer ID, (6.1, 6.2, 6.n) entschieden. Dazu weist das Zugangssystem (3.1, 3.2, 3.n) eine Datenverarbeitungseinrichtung (7.1, 7.2, 7.n) und eine Speichereinrichtung (8.1, 8.2, 8.n) auf. In der jeweiligen Speichereinrichtung (8.1, 8.2, 8.n) ist eine dem jeweiligen Müllaufnahmebehältnis (2.1, 2.2, 2.n) zugeordnete individuelle Sperrliste abgespeichert, in der diejenigen Schlüssel (6.1, 7.2, 6.n) enthalten sind, denen der Zugang zu diesem Müllaufnahmebehältnis (2.1, 2.2, 2.n) verweigert werden soll.

[0049] Wird dagegen durch den Benutzer ein Schlüssel (6.1, 7.2, 6.n) verwendet, der nicht in der individuellen Sperrliste dieses Müllaufnahmebehältnisses (2.1, 2.2, 2.n) enthalten ist, wird über eine ebenfalls im Zugangssystem (3.1, 3.2, 3.n) enthaltene Steuerungseinrichtung (9.1, 9.2, 9.n) die Verriegelungseinrichtung (5.1, 5.2, 5.n) entriegelt und der Zugang zur Schleuseneinrichtung (4.1, 4.2, 4.n) für den Benutzer freigegeben, so dass er Müll durch die Schleuseneinrichtung (4.1, 4.2, 4.n) in das Müllaufnahmebehältnis (2.1, 2.2, 2.n) einwerfen kann.

[0050] Der Schlüssel (6.1, 7.2, 6.n) des Benutzers wird von dem jeweiligen Zugangssystem (3.1, 3.2, 3.n) über eine Kommunikationsschnittstelle (10.1, 10.2, 10.n) eingelesen. Bei dem Schlüssel (6.1, 7.2, 6.n) kann es sich beispielsweise um eine Chipkarte, einen RFID-Tag oder ein Mobiltelefon handeln. Bevorzugt ist die Kommunikationsschnittstelle (10.1, 10.2, 10.n) zur drahtlosen Kommunikation geeignet.

[0051] In der dargestellten Ausführungsform weist das Zugangssystem (3.1, 3.2, 3.n) jedes Müllaufnahmebehältnisses (2.1, 2.2, 2.n) weiterhin eine Lokalisierungseinrichtung (11.1, 11.2, 11.n) und eine Zeiterfassungseinrichtung (12.1, 12.2, 12.n) auf. Mittels der Lokalisierungseinrichtung (11.1, 11.2, 11.n) kann der aktuelle Standort des jeweiligen Müllaufnahmebehältnisses (2.1, 2.2, 2.n) bestimmt beispielsweise mittels NAVSTAR GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo oder Beidou oder eine Kombination verschiedener Systeme ermittelt werden. Die Zeiterfassungseinrichtung (12.1, 12.2, 12.n) kann dazu verwendet werden, jedem Nutzungsversuch eines Benutzers einen eindeutigen Zeitstempel zuzuordnen, so dass jeder Nutzungsversuch für jedes Müllaufnahmebehältnis (2.1, 2.2, 2.n) sowohl örtlich als auch zeitlich dokumentierbar ist. Ergänzend dazu oder als Alternative könnte die Standortermittlung des Zugangssystems auch zum Zeitpunkt der Inbetriebnahme oder Wartung vor Ort mittels eines Service-tools (z.B. Smartphone App) erfolgen, das GPS-Daten erfassen kann und die Standortdaten des Zugangssystems bzw. des Müllaufnahmebehältnis entweder direkt in das Datenmanage-

mentsystem oder im Zugangs-system hinterlegt. Das Zugangssystem kann diese Daten dann über Funk an das Datenmanagementsystem übertragen.

[0052] Die Kommunikationsschnittstelle (10.1, 10.2, 10.n) dient auch der Datenübertragung zu und von dem Datenmanagementsystem (1). Dazu weist die Kommunikationsschnittstelle (10.1, 10.2, 10.n) bevorzugt einen separaten Kommunikationskanal auf. Dieser unterscheidet sich bevorzugt von demjenigen, mittels dem der Schlüssel eines Benutzers eingelesen wird. Die beiden Kommunikationskanäle der Kommunikationsschnittstelle (10.1, 10.2, 10.n) können auch als separate Untereinheiten ausgeführt sei, die räumlich voneinander entfernt in oder an dem Müllaufnahmebehältnis (2.1, 2.2, 2.n) und/oder dem Zugangssystem (3.1, 3.2, 3.n) angeordnet sein.

[0053] Die Kommunikationsschnittstelle (10.1, 10.2, 10.n) ist bevorzugt zur drahtlosen Kommunikation mit dem Datenmanagementsystem (1) ausgelegt. Dies hat den Vorteil, dass die Daten nicht händisch (beispielsweise mittels eines USB-Stick) durch Bedienpersonal ausgetauscht werden müssen. Bevorzugt wird zum Datenaustausch zwischen der Kommunikationsschnittstelle (10.1, 10.2, 10.n) und dem Datenmanagementsystem (1) eine Mobilfunkverbindung genutzt.

[0054] Figur 2 zeigt eine Prinzipskizze des elektronischen Sperrlistenverwaltungssystems für die Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses nach einer Ausführungsform. Wie in dieser Prinzipskizze dargestellt ist, wird in einem Schritt (21) eine Liste aller nicht zugangsberechtigten Schlüssel angelegt. Ist diese Liste so lang, dass mit verzögerter Authentifizierung von Schlüsseln an dem Zugangssystem (3.1, 3.2, 3.n) der jeweiligen Müllaufnahmebehältnisse (2.1, 2.2, 2.n) gerechnet werden muss, wird in Schritt 22 eine maximale Anzahl x von Einträgen pro Sperrliste (Blacklist) festgelegt. Wenn diese Anzahl x geringer ist als die Anzahl aller Einträge in der Liste der nicht zugangsberechtigten Schlüssel, ist es in Schritt (23) erforderlich Kriterien festzulegen, mittels denen ein Priorisierungsalgorithmus eine Priorisierungsrangfolge nicht zugangsberechtigter Schlüssel festlegen kann.

[0055] Für eine effektive Zugangskontrolle zu einem bestimmten Müllaufnahmebehältnis (z.B. 2.1 aus einer Vielzahl von Müllaufnahmebehältnissen (2.1, 2.2, 2.n) zu ermöglichen, werden zunächst in Schritt (24) alle Zugangsversuche aller Schlüssel an jedem Zugangssystem (3.1, 3.2, 3.n) des Systems erkannt und in Schritt (25) für einen festgelegten Zeitraum in der Speichereinrichtung des Zugangssystems (3.1, 3.2, 3.n) gespeichert.

[0056] In Schritt (26) werden die in einem oder mehreren Zugangssystemen (3.1, 3.2, 3.n) gespeicherten Daten über Zugangsversuche an das Datenmanagementsystem (1) übertragen. Diese Übertragung kann in regelmäßigen Intervallen, benutzerinitiiert oder bei Überschreiten (z.B. > 75 %, bevorzugt > 80 %, besonders bevorzugt > 90 %) einer vorgegebenen Speicherauslastung der Speichereinrichtung (8.1, 8.2, 8.n) des jeweili-

gen Zugangssysteme (3.1, 3.2, 3.n) erfolgen. Nach der Übertragung können die übertragenen Daten in dem Datenmanagementsystem (1) gespeichert und archiviert werden, so dass die Speichereinrichtung (8.1, 8.2, 8.n) des jeweiligen Zugangssystems (3.1, 3.2, 3.n) zur Speicherung neuer Daten über Zugangsversuche geleert werden kann.

[0057] Sind die Daten über Zugangsversuche an das Datenmanagementsystem (1) übertragen, kann dort in Schritt (27) die Erstellung einer Priorisierungsrangfolge für die nicht zugangsberechtigten Schlüssel für jedes Zugangssystem (3.1, 3.2, 3.n) auf Basis des zuvor festgelegten Priorisierungsalgorithmus (siehe Schritt 23) erfolgen. Da sich die Daten über Zugangsversuche an den verschiedenen Müllaufnahmebehältnissen (2.1, 2.2, 2.n) unterscheiden, ergibt sich für jedes Müllaufnahmebehältnis (2.1, 2.2, 2.n) auf Basis der Zugangsversuche und des zugrundeliegenden Priorisierungsalgorithmus eine individuelle Priorisierungsrangfolge. Insbesondere bei größeren Systemen mit sehr vielen Müllaufnahmebehältnissen (2.1, 2.2, 2.n) ist daher ein vergleichsweise großer Rechenaufwand zu erwarten.

[0058] Auf Basis der individuellen Priorisierungsrangfolge wird in Schritt (28) für jedes Müllaufnahmebehältnis (2.1, 2.2, 2.n) eine individuelle Sperrliste (Blacklist) erzeugt. Diese ist auf eine Anzahl von x Einträgen begrenzt, um die Datenverarbeitung durch das Zugangssystem (3.1, 3.2, 3.n) vor Ort möglichst gering zu halten. Einträge, deren Position in der Priorisierungsrangfolge die Anzahl x überschreitet, werden nicht in die Sperrliste aufgenommen.

[0059] Nach der Erzeugung der Sperrlisten erfolgt in Schritt (29) die Übertragung der individuellen Sperrliste an das jeweilige Zugangssystem (3.1, 3.2, 3.n). Je nach zur Verfügung stehender Bandbreite des Übertragungsnetzes kann dies gemeinsam für alle Sperrlisten und Zugangssysteme (3.1, 3.2, 3.n) gleichzeitig erfolgen oder lediglich für einzelne Zugangssysteme (3.1, 3.2, 3.n) oder eine Gruppe von Zugangssystemen (3.1, 3.2, 3.n).

[0060] Nach der Übertragung steht die jeweilige Sperrliste in dem entsprechenden Zugangssystem (3.1, 3.2, 3.n) zur Bewertung der Zugangsberechtigung für Nutzer eines bestimmten Schlüssels zu Verfügung. Ist der Schlüssel, mit dem ein Benutzer Zugang zum Müllaufnahmebehältnis (2.1, 2.2, 2.n) anfragt in der Sperrliste des Zugangssystems (3.1, 3.2, 3.n) dieses Müllaufnahmebehältnisses (2.1, 2.2, 2.n) enthalten, wird der Zugang zum Müllaufnahmebehältnis (2.1, 2.2, 2.n) verweigert und die Verriegelungseinrichtung (5.1, 5.2, 5.n) bleibt verriegelt.

[0061] Figur 3 zeigt eine beispielhafte Darstellung für die Erstellung einer Priorisierungsrangfolge und einer daraus resultierenden individuellen Sperrliste. Im linken Bereich (Spalten 1 und 2) sind alle an das Datenmanagementsystem (1) übertragenen Daten über Zugangsversuche an einem bestimmten Müllaufnahmebehältnis über einen Zeitraum von einigen aufeinanderfolgenden Tagen dargestellt. Die jeweiligen Datensätze enthalten einen

Zeitstempel und eine Schlüssel-ID. Die Datensätze enthalten sowohl Zugangsversuche zugelassener Schlüssel als auch (in diesem Fall zweier) nicht zugelassener Schlüssel (Schlüssel-ID fett hervorgehoben).

[0062] Im Datenmanagementsystem (1) sind für jeden Zeitabschnitt (in diesem Fall A, B, C und D) bestimmte Gewichtungsfaktoren hinterlegt (in diesem Fall 10, 8, 6 und 4). Im gezeigten Beispiel wird jedem der Zugangsversuche mit einem nicht zugelassenen Schlüssel der dem jeweiligen Zeitabschnitt zugeordnete Gewichtungsfaktor zugewiesen. Das Produkt aus Anzahl der Zugangsversuche pro Zeitabschnitt und dem jeweiligen Gewichtungsfaktor ergibt für jeden Zeitabschnitt und jeden nicht zugelassenen Schlüssel einen Wert. Summiert man die Werte für jeden Schlüssel einzeln auf, ergibt die Summe einen Gewichtungswert, anhand dessen die Priorisierung erfolgen kann. Im vorliegenden Beispiel wird aufgrund der ermittelten Summe von 46 der Schlüssel A8E1AD06 höher priorisiert als der Schlüssel 5CA3DA03, der lediglich auf eine Summe von 28 kam.

[0063] Die hier exemplarisch dargestellten Werte für die Gewichtung dienen lediglich der Veranschaulichung. Die Gewichtung kann den jeweiligen Bedürfnissen angepasst werden. Darüber hinaus kann das System auch durch weitere Gewichtungsfaktoren optimiert werden. Beispielsweise kann, zwischen bei nicht zugangsberechtigten Schlüsseln, auch der Grund des Entzugs der Zugangsberechtigung in die Gewichtung einfließen.

[0064] Wurde beispielsweise ein Schlüssel verloren und ein anderer verliert aufgrund des Auszugs eines Bewohners die Zugangsberechtigung, könnte bei dem verlorenen Schlüssel aufgrund des unklaren Benutzers und einer höheren Wahrscheinlichkeit eines illegalen Gebrauchs eine höhere Gewichtung vorteilhaft sein, während der ausgezogene Bewohner weiterhin identifizierbar ist und so eventuelle Nutzungsgebühren des Müllaufnahmebehältnis weiterhin einforderbar sind.

[0065] Außerdem könnten beispielsweise Zeitstempel unberechtigter Schlüssel, die noch immer benutzt werden höher gewichtet werden als solche die nicht mehr verwendet werden und/oder unberechtigte Zeitstempel (z.B. nach Verlust des Schlüssels) höher gewichtet werden als berechtigte Zeitstempel (also vor Verlust des Schlüssels).

Bezugszeichenliste

[0066]

1	Datenmanagementsystem
2.1, 2.2, 2.n	Müllaufnahmebehältnisse
3.1, 3.2, 3.n	Zugangssystem
4.1, 4.2, 4.n	Schleuseneinrichtung
5.1, 5.2, 5.n	Verriegelungseinrichtung
6, 6.1, 6.2, 6.n	Schlüssel, ID
7.1, 7.2, 7.n	Datenverarbeitungseinrichtung
8.1, 8.2, 8.n	Speichereinrichtung
9.1, 9.2, 9.n	Steuerungseinrichtung

10.1, 10.2, 10.n	Kommunikationsschnittstelle
11.1, 11.2, 11.n	Lokalisierungseinrichtung
12.1, 12.2, 12.n	Zeiterfassungseinrichtung
21-30	Schritt

5

Patentansprüche

1. Elektronisches Sperrlistenverwaltungssystem für eine Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehältnisses (2.1, 2.2, 2.n), wobei das Sperrlistenverwaltungssystem ein Datenmanagementsystem (1) und eine Vielzahl von mittels einer Vielzahl von Schlüsseln (6), die jeweils einem Benutzer oder einer Benutzergruppe zuordenbar sind, aktivierbaren Zugangssystemen (3.1, 3.2, 3.n) für eine elektronische Berechtigungskontrolle zur Benutzung eines jedem einzelnen Zugangssystem (3.1, 3.2, 3.n) zugeordneten einzelnen Müllaufnahmebehältnisses (2.1, 2.2, 2.n) umfasst, wobei sowohl das Datenmanagementsystem (1) als auch jedes der Zugangssysteme (3.1, 3.2, 3.n) eine Kommunikationsschnittstelle (10.1, 10.2, 10.n) aufweisen, mittels der Daten zwischen dem Datenmanagementsystem (1) und jedem einzelnen Zugangssystem (3.1, 3.2, 3.n) austauschbar sind, wobei jedes Zugangssystem (3.1, 3.2, 3.n) eine Speichereinrichtung (8.1, 8.2, 8.n) zum Erstellen und Speichern einer Liste der in einem festgelegten Zeitraum an diesem Zugangssystem (3.1, 3.2, 3.n) verwendeten Schlüssel (6, 6.1, 6.2, 6.n) und Mittel zur Übertragung dieser Liste mittels der Kommunikationsschnittstelle (10.1, 10.2, 10.n) an das Datenmanagementsystem (1) aufweist, und das Datenmanagementsystem (1) Einrichtungen zum Erstellen einer Sperrliste für das Zugangssystem (3.1, 3.2, 3.n) eines Müllaufnahmebehältnisses (2.1, 2.2, 2.n) aufweist, wobei

- das Datenmanagementsystem (1) dazu eingerichtet ist, beim Erstellen der Sperrliste auf einen Priorisierungsalgorithmus zur Priorisierung von Einträgen in der Sperrliste zurückzugreifen, wobei der Priorisierungsalgorithmus zumindest auch das Merkmal der letzten Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an dem Zugangssystem (3.1, 3.2, 3.n) des jeweiligen Müllaufnahmebehältnisses (2.1, 2.2, 2.n) berücksichtigt, um jeweils eine individuelle Priorisierungsrangfolge aller nicht zugangsberechtigten Schlüssel (6, 6.1, 6.2, 6.n) für das Zugangssystem (3.1, 3.2, 3.n) jedes einzelnen definierten Müllaufnahmebehältnisses (2.1, 2.2, 2.n) durch das Datenmanagementsystem (1) zu erstellen, wobei durch das Datenmanagementsystem (1) die nicht zugangsberechtigten Schlüssel (6, 6.1, 6.2, 6.n) beginnend mit dem Schlüssel (6, 6.1, 6.2, 6.n) mit der höchsten Priorisierung in absteigender Rangfolge der Pri-

orisierung in die individuelle Sperrliste des Zugangssystems (3.1, 3.2, 3.n) jedes einzelnen definierten Müllaufnahmebehältnisses (2.1, 2.2, 2.n) aufgenommen werden, bis die maximale Anzahl der Sperrlisteneinträge erreicht ist, - jedes Zugangssystem (3.1, 3.2, 3.n) eine Speichereinrichtung (8.1, 8.2, 8.n) zum Speichern der vom Datenmanagementsystem (1) erstellten und von diesem an das jeweilige Zugangssystem (3.1, 3.2, 3.n) übertragenen Sperrliste für das diesem Zugangssystem (3.1, 3.2, 3.n) zugeordneten Müllaufnahmebehältnisses (2.1, 2.2, 2.n) aufweist und jedes Zugangssystem (3.1, 3.2, 3.n) eine Datenverarbeitungseinrichtung (7.1, 7.2, 7.n) und eine Steuerungseinrichtung (9.1, 9.2, 9.n) zum Gewähren oder Verweigern des Zugangs zu dem dem Zugangssystem (3.1, 3.2, 3.n) zugeordneten Müllaufnahmebehältnis (2.1, 2.2, 2.n) für einen dem Schlüssel (6, 6.1, 6.2, 6.n) zugeordneten Benutzer umfasst, wobei eine Zugangsverweigerung eine Folge eines erfolgreichem Abgleich des Schlüssels (6, 6.1, 6.2, 6.n) mit den in der individuellen Sperrliste des Zugangssystems (3.1, 3.2, 3.n) dieses definierten Müllaufnahmebehältnisses (2.1, 2.2, 2.n) enthaltenden Einträgen ist.

2. Elektronisches Sperrlistenverwaltungssystem nach Anspruch 1, **dadurch gekennzeichnet, dass** der Priorisierungsalgorithmus Rechenvorschriften umfasst, die mindestens ein Merkmal abbilden, das ausgewählt ist aus einer Gruppe bestehend aus:

- der Häufigkeit der Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an dem Zugangssystem (3.1, 3.2, 3.n) des jeweiligen Müllaufnahmebehältnisses (2.1, 2.2, 2.n),
- der letzten Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an einem Zugangssystem (3.1, 3.2, 3.n) eines anderen Müllaufnahmebehältnisses (2.1, 2.2, 2.n), welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnisses (2.1, 2.2, 2.n) angeordnet ist,
- der Häufigkeit der letzten Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an einem Zugangssystem (3.1, 3.2, 3.n) eines anderen Müllaufnahmebehältnisses (2.1, 2.2, 2.n), welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnis (2.1, 2.2, 2.n) angeordnet ist,
- der Höhe eines ausstehenden Rechnungsbetrags des diesem Schlüssel (6, 6.1, 6.2, 6.n) zugeordneten Benutzers und
- der geographischen Verteilung der Nutzung eines nicht zugangsberechtigten Schlüssels (6,

- 6.1, 6.2, 6.n) an einem Zugangssystem (3.1, 3.2, 3.n) anderer Müllaufnahmebehälter (2.1, 2.2, 2.n).
3. Elektronisches Sperrlistenverwaltungssystem nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** zumindest eines der Zugangssysteme (3.1, 3.2, 3.n), bevorzugt eine Vielzahl von Zugangssystemen (3.1, 3.2, 3.n), weiter bevorzugt alle Zugangssysteme (3.1, 3.2, 3.n), eine Einrichtung zum Ausschluss eines Schlüssels (6, 6.1, 6.2, 6.n) zu allen Zugangssystemen (3.1, 3.2, 3.n) des elektronischen Sperrlistenverwaltungssystems aufweist. 5 10
 4. Elektronisches Sperrlistenverwaltungssystem nach Anspruch 3, **dadurch gekennzeichnet, dass** die Einrichtung zum Ausschluss eines Schlüssels (6, 6.1, 6.2, 6.n) zu allen Zugangssystemen (3.1, 3.2, 3.n) des elektronischen Sperrlistenverwaltungssystems eine Vorrichtung zum Einziehen des Schlüssels (6, 6.1, 6.2, 6.n) oder zum Löschen, Überschreiben oder anderwärtig Unbrauchbarmachen einer auf dem Schlüssel (6, 6.1, 6.2, 6.n) gespeicherten Identifikationsnummer ist. 20 25
 5. Elektronisches Sperrlistenverwaltungssystem nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die Kommunikationsschnittstelle (10.1, 10.2, 10.n) zum Austausch der Daten zwischen dem Datenmanagementsystem (1) und jedem einzelnen Zugangssystem (3.1, 3.2, 3.n) eine zur drahtlosen Kommunikation geeignete Kommunikationsschnittstelle (10.1, 10.2, 10.n) ist, welche bevorzugt eine Mobilfunkkommunikationseinrichtung ist, welche insbesondere bevorzugt ausgewählt ist aus einer Gruppe bestehend aus einer GSM-, einer UMTS-, einer GPRS- und einer LTE-Mobilfunkkommunikationseinrichtung. 30 35 40
 6. Elektronisches Sperrlistenverwaltungssystem nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Zugangssystem eine Schleuseneinrichtung (4.1, 4.2, 4.n) mit einer Verriegelungseinrichtung (5.1, 5.2, 5.n) aufweist, wobei die Steuerungseinrichtung (9.1, 9.2, 9.n) ein Freigabesignal zum Entriegeln der Verriegelungseinrichtung (5.1, 5.2, 5.n) abgibt, wenn der Abgleich des Schlüssels (6, 6.1, 6.2, 6.n) mit den in der Sperrliste enthaltenen Einträgen in der Datenverarbeitungseinrichtung (7.1, 7.2, 7.n) negativ ist. 45 50
 7. Elektronisches Sperrlistenverwaltungssystem nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Zugangssystem (3.1, 3.2, 3.n) und/oder ein Müllaufnahmebehälter (2.1, 2.2, 2.n) eine Lokalisierungseinrichtung (11.1, 11.2, 11.n) aufweist, durch welche der aktuelle Standort des Müllaufnahmebehälters (2.1, 2.2, 2.n), bevorzugt mittels eines globalen Navigationssatellitensystems, insbesondere bevorzugt ausgewählt aus einer Gruppe, die NAVSTAR GPS (Global Positioning System), GLO-NASS (Global Navigation Satellite System), Galileo und Beidou umfasst, ermittelbar ist, wobei der Standort an das Datenmanagementsystem (1) übertragbar ist, bevorzugt über die Kommunikationsschnittstelle (10.1, 10.2, 10.n).
 8. Verfahren zur Datenverwaltung einer Sperrliste in einem Zugangssystem für eine elektronische Berechtigungskontrolle zur Benutzung eines Müllaufnahmebehälters (2.1, 2.2, 2.n) mit den Schritten
 - a. Festlegen einer maximalen Anzahl der Sperrlisteneinträge,
 - b. Übertragung der in einem festgelegten Zeitraum an dem Zugangssystem (3.1, 3.2, 3.n) jedes einzelnen Müllaufnahmebehälters (2.1, 2.2, 2.n) aus einer Vielzahl von Müllaufnahmebehältern (2.1, 2.2, 2.n) bisher verwendeten Schlüssel (6, 6.1, 6.2, 6.n) an ein Datenmanagementsystem (1),
 - c. Sofern die maximale Anzahl der Sperrlisteneinträge noch nicht erreicht ist: Aufnahme der nicht zugangsberechtigten Schlüssel (6, 6.1, 6.2, 6.n) in die Sperrliste und Übertragung der Sperrliste an die Zugangssysteme (3.1, 3.2, 3.n) aller Müllaufnahmebehälter (2.1, 2.2, 2.n) durch das Datenmanagementsystem (1), oder falls die maximale Anzahl der Sperrlisteneinträge erreicht ist:
 - d. Festlegen eines Priorisierungsalgorithmus zur Priorisierung von Einträgen in einer Sperrliste für das Zugangssystem (3.1, 3.2, 3.n) eines Müllaufnahmebehälters (2.1, 2.2, 2.n), wobei der Priorisierungsalgorithmus zumindest auch das Merkmal der letzten Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an dem Zugangssystem des jeweiligen Müllaufnahmebehälters (2.1, 2.2, 2.n) berücksichtigt,
 - e. Erstellen jeweils einer individuellen Priorisierungsrangfolge aller nicht zugangsberechtigten Schlüssel (6, 6.1, 6.2, 6.n) für das Zugangssystem (3.1, 3.2, 3.n) jedes einzelnen definierten Müllaufnahmebehälters (2.1, 2.2, 2.n) durch das Datenmanagementsystem (1),
 - f. Aufnahme der nicht zugangsberechtigten Schlüssel (6, 6.1, 6.2, 6.n) beginnend mit dem Schlüssel (6, 6.1, 6.2, 6.n) mit der höchsten Priorisierung in absteigender Rangfolge der Priorisierung in die individuelle Sperrliste des Zugangssystems (3.1, 3.2, 3.n) jedes einzelnen

- definierten Müllaufnahmebehältnisses (2.1, 2.2, 2.n) bis die maximale Anzahl der Sperrlisteneinträge erreicht ist durch das Datenmanagementsystem (1),
- g. Übertragung der individuellen Sperrliste an das Zugangssystem (3.1, 3.2, 3.n) des jeweiligen Müllaufnahmebehältnisses (2.1, 2.2, 2.n),
- h. Gewährung oder Verweigerung des Zugangs zu einem definierten Müllaufnahmebehältnis gemäß der in der individuellen Sperrliste des Zugangssystems (3.1, 3.2, 3.n) des jeweiligen definierten Müllaufnahmebehältnisses (2.1, 2.2, 2.n) hinterlegten Schlüssel (6, 6.1, 6.2, 6.n).
9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass
der Priorisierungsalgorithmus weiterhin Merkmal berücksichtigt, die ausgewählt sind aus einer Gruppe bestehend aus
- der Häufigkeit der Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an dem Zugangssystem (3.1, 3.2, 3.n) des jeweiligen Müllaufnahmebehältnisses (2.1, 2.2, 2.n),
 - der letzten Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an einem Zugangssystem (3.1, 3.2, 3.n) eines anderen Müllaufnahmebehältnisses (2.1, 2.2, 2.n), welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnis (2.1, 2.2, 2.n) angeordnet ist,
 - der Häufigkeit der letzten Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an einem Zugangssystem (3.1, 3.2, 3.n) eines anderen Müllaufnahmebehältnisses (2.1, 2.2, 2.n), welches geographisch in einem vordefinierten Abstand vom jeweiligen Müllaufnahmebehältnis (2.1, 2.2, 2.n) angeordnet ist,
 - der Höhe eines ausstehenden Rechnungsbetrags des diesem Schlüssel (6, 6.1, 6.2, 6.n) zugeordneten Benutzers und
 - der geographischen Verteilung der Nutzung eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) an einem Zugangssystem (3.1, 3.2, 3.n) anderer Müllaufnahmebehältnisse (2.1, 2.2, 2.n).
10. Verfahren nach Anspruch 8 oder 9,
dadurch gekennzeichnet, dass
bei der Überschreitung einer festgelegten Anzahl von abgelehnten Zugangsversuchen eines nicht zugangsberechtigten Schlüssels (6, 6.1, 6.2, 6.n) der Schlüssel (6, 6.1, 6.2, 6.n) durch das Zugangssystem (3.1, 3.2, 3.n) von der weiteren Nutzung ausgeschlossen wird.
11. Verfahren nach Anspruch 10,
- dadurch gekennzeichnet, dass**
das Zugangssystem (3.1, 3.2, 3.n) den Schlüssel (6, 6.1, 6.2, 6.n) einzieht oder eine auf dem Schlüssel (6, 6.1, 6.2, 6.n) gespeicherte Identifikationsnummer löscht, überschreibt oder anderwärtig unbrauchbar macht.
12. Verfahren nach einem der Ansprüche 8 bis 11,
dadurch gekennzeichnet, dass
die Datenverarbeitung durch das Datenmanagementsystem (1) örtlich von dem jeweiligen Müllaufnahmebehältnis (2.1, 2.2, 2.n) getrennt vorgenommen wird.
13. Verfahren nach Anspruch 12,
dadurch gekennzeichnet, dass
die Übertragung von Daten zwischen einem Zugangssystem (3.1, 3.2, 3.n) eines Müllaufnahmebehältnisses (2.1, 2.2, 2.n) und dem Datenmanagementsystem (1) drahtlos erfolgt.
14. Verfahren nach Anspruch 12 oder 13,
dadurch gekennzeichnet, dass
die Übertragung von Daten zwischen einem Zugangssystem (3.1, 3.2, 3.n) eines Müllaufnahmebehältnisses (2.1, 2.2, 2.n) und dem Datenmanagementsystem (1) mittels einer Mobilfunkverbindung erfolgt, welche bevorzugt ausgewählt ist aus einer Gruppe bestehend aus einer GSM-Verbindung, einer UMTS-Verbindung, einer GPRS-Verbindung und einer LTE-Verbindung.
15. Verfahren nach einem der Ansprüche 8 bis 14,
dadurch gekennzeichnet, dass
die Schritte b, e, f und g periodisch wiederholend vorgenommen werden, wobei die Wiederholung bevorzugt in einem Intervall erfolgt, welches ausgewählt ist aus einer Gruppe, die tägliche, wöchentliche, monatliche, quartalsweise, halbjährliche oder jährliche Wiederholung umfasst.

Claims

1. An electronic blocking list management system for checking authorisation to use a rubbish receptacle (2.1, 2.2, 2.n), wherein the blocking list management system comprises a data management system (1) and multiple access systems (3.1, 3.2, 3.n), which can be activated by means of multiple keys (6), which are each assigned to a user or a group of users, for electronically checking authorisation to use an individual rubbish receptacle (2.1, 2.2, 2.n) associated with any individual access system (3.1, 3.2, 3.n), wherein both the data management system (1) and each of the access systems (3.1, 3.2, 3.n) have a communication interface (10.1, 10.2, 10.n), by means of which data can be exchanged between the

data management system (1) and each individual access system (3.1, 3.2, 3.n), wherein each access system (3.1, 3.2, 3.n) has a memory device (8.1, 8.2, 8.n) for creating and storing a list of the keys (6, 6.1, 6.2, 6.n) used in a defined period of time at this access system (3.1, 3.2, 3.n) and means for transmitting this list by means of the communication interface (10.1, 10.2, 10.n) to the data management system (1), and the data management system (1) has devices for creating a blocking list for the access system (3.1, 3.2, 3.n) of a rubbish receptacle (2.1, 2.2, 2.n), wherein

- the data management system (1) is configured to access a prioritisation algorithm for prioritising entries in the blocking list when creating the blocking list, wherein the prioritisation algorithm at least also takes into consideration the feature of the last use of a key (6, 6.1, 6.2, 6.n) not authorised for access at the access system (3.1, 3.2, 3.n) of the respective rubbish receptacle (2.1, 2.2, 2.n) to create, by means of the data management system (1), respectively, an individual prioritisation hierarchy for all keys (6, 6.1, 6.2, 6.n) not authorised for access for the access system (3.1, 3.2, 3.n) of each individual defined rubbish receptacle (2.1, 2.2, 2.n), wherein, by means of the data management system (1), the keys (6, 6.1, 6.2, 6.n) not authorised for access, starting with the key (6, 6.1, 6.2, 6.n) with the highest prioritisation in descending hierarchy of the prioritisation, in the individual blocking list of the access system (3.1, 3.2, 3.n) of each individual defined rubbish receptacle (2.1, 2.2, 2.n) are included until the maximum number of blocking list entries is reached,

- each access system (3.1, 3.2, 3.n) has a memory device (8.1, 8.2, 8.n) for storing the blocking list created by the data management system (1) and transmitted therefrom to the respective access system (3.1, 3.2, 3.n) for the rubbish receptacle (2.1, 2.2, 2.n) associated with this access system (3.1, 3.2, 3.n), and each access system (3.1, 3.2, 3.n) comprises a data processing device (7.1, 7.2, 7.n) and a control device (9.1, 9.2, 9.n) for granting or refusing access to the rubbish receptacle (2.1, 2.2, 2.n) associated with the access system (3.1, 3.2, 3.n) for a user associated with the key (6, 6.1, 6.2, 6.n), wherein access refusal results from a successful comparison of the key (6, 6.1, 6.2, 6.n) with the entries contained in the individual blocking list of the access system (3.1, 3.2, 3.n) of this defined rubbish receptacle (2.1, 2.2, 2.n).

2. The electronic blocking list management system according to claim 1, **characterised in that**

the prioritisation algorithm comprises computing specifications which display at least one feature selected from the group consisting of:

- the frequency of use of a key (6, 6.1, 6.2, 6.n) not authorised for access at the access system (3.1, 3.2, 3.n) of the respective rubbish receptacle (2.1, 2.2, 2.n),
- the last use of a key (6, 6.1, 6.2, 6.n) not authorised for access at an access system (3.1, 3.2, 3.n) of another rubbish receptacle (2.1, 2.2, 2.n) which is arranged geographically at a predefined distance from the respective rubbish receptacle (2.1, 2.2, 2.n),
- the frequency of the last use of a key (6, 6.1, 6.2, 6.n) not authorised for access at an access system (3.1, 3.2, 3.n) of another rubbish receptacle (2.1, 2.2, 2.n) arranged geographically at a predefined distance from the respective rubbish receptacle (2.1, 2.2, 2.n),
- the value of an outstanding invoice amount owed by the user associated with this key (6, 6.1, 6.2, 6.n), and
- the geographic distribution of the use of a key (6, 6.1, 6.2, 6.n) not authorised for access at an access system (3.1, 3.2, 3.n) of other rubbish receptacles (2.1, 2.2, 2.n).

3. The electronic blocking list management system according to claim 1 or 2, **characterised in that** at least one of the access systems (3.1, 3.2, 3.n), preferably a plurality of access systems (3.1, 3.2, 3.n), more preferably all access systems (3.1, 3.2, 3.n) has/have a device for excluding a key (6, 6.1, 6.2, 6.n) with respect to all access systems (3.1, 3.2, 3.n) of the electronic blocking list management system.
4. The electronic blocking list management system according to claim 3, **characterised in that** the device for excluding a key (6, 6.1, 6.2, 6.n) with respect to all access systems (3.1, 3.2, 3.n) of the electronic blocking list management system is an apparatus for confiscating the key (6, 6.1, 6.2, 6.n) or for deleting, overwriting or otherwise making unusable an identification number stored on the key (6, 6.1, 6.2, 6.n).
5. The electronic blocking list management system according to any of the preceding claims, **characterised in that** the communication interface (10.1, 10.2, 10.n) for exchanging data between the data management system (1) and each individual access system (3.1, 3.2, 3.n) is a communication interface (10.1, 10.2, 10.n) suitable for wireless communication, which is

preferably a mobile communication device, which is particularly preferably selected from a group consisting of a GSM, UMTS, GPRS and LTE mobile communication device.

6. The electronic blocking list management system according to any of the preceding claims, **characterised in that**
 - an access system has a port device (4.1, 4.2, 4.n) with a locking device (5.1, 5.2, 5.n), wherein the control device (9.1, 9.2, 9.) emits a release signal for unlocking the locking device (5.1, 5.2, 5.n) if the comparison of the key (6, 6.1, 6.2, 6.n) with the entries contained in the blocking list is negative in the data processing device (7.1, 7.2, 7.n).
7. The electronic blocking list management system according to any of the preceding claims, **characterised in that**
 - an access system (3.1, 3.2, 3.n) and/or a rubbish receptacle (2.1, 2.2, 2.n) has a locating device (11.1, 11.2, 11.n), by means of which the current location of the rubbish receptacle (2.1, 2.2, 2.n) can be determined, preferably by means of a global navigation satellite system, particularly preferably selected from the group comprising NAVSTAR GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo and Beidou, wherein the location can be transmitted to the data management system (1), preferably via the communication interface (10.1, 10.2, 10.n).
8. A method for data management of a blocking list in an access system for electronically checking authorisation to use a rubbish receptacle (2.1, 2.2, 2.n), with the following steps
 - a. defining a maximum number of blocking list entries,
 - b. transmitting to a data management system (1) the key (6, 6.1, 6.2, 6.n) used previously within a defined period of time at the access system (3.1, 3.2, 3.n) of any individual rubbish receptacle (2.1, 2.2, 2.n) from multiple rubbish receptacle containers (2.1, 2.2, 2.n),
 - c. if the maximum number of blocking list entries is not reached: including the key (6, 6.1, 6.2, 6.n) not authorised for access in the blocking list and transmitting the blocking list to the access systems (3.1, 3.2, 3.n) of all rubbish receptacles (2.1, 2.2, 2.n) by means of the data management (1) system, or if the maximum number of blocking list entries is reached,
 - d. defining a prioritisation algorithm for prioritising entries in a blocking list for the access system (3.1, 3.2, 3.n) of a rubbish receptacle (2.1, 2.2, 2.n), wherein the prioritisation algorithm at least also takes into consideration the feature of the

last use of a key (6, 6.1, 6.2, 6.n) not authorised for access at the access system of the respective rubbish receptacle (2.1, 2.2, 2.n),
 e. creating, by means of the data management system (1), an individual prioritisation hierarchy for all keys (6, 6.1, 6.2, 6.n) not authorised for access for the access system (3.1, 3.2, 3.n) of each individual defined rubbish receptacle (2.1, 2.2, 2.n),
 f. including, by means of the data management system (1), the keys (6, 6.1, 6.2, 6.n) not authorised for access, starting with the key (6, 6.1, 6.2, 6.n) with the highest prioritisation in descending hierarchy of the prioritisation, in the individual blocking list of the access system (3.1, 3.2, 3.n) of each individual defined rubbish receptacle (2.1, 2.2, 2.n) until the maximum number of blocking list entries is reached,
 g. transmitting the individual blocking list to the access system (3.1, 3.2, 3.n) of the respective rubbish receptacle (2.1, 2.2, 2.n), and
 h. granting or refusing access to a defined rubbish receptacle in accordance with the keys (6, 6.1, 6.2, 6.n) stored in the individual blocking list of the access system (3.1, 3.2, 3.n) of the respective defined rubbish receptacle (2.1, 2.2, 2.n).

9. The method according to claim 8, **characterised in that** the prioritisation algorithm also takes into consideration features selected from the group consisting of
 - the frequency of use of a key (6, 6.1, 6.2, 6.n) not authorised for access at the access system (3.1, 3.2, 3.n) of the respective rubbish receptacle (2.1, 2.2, 2.n),
 - the last use of a key (6, 6.1, 6.2, 6.n) not authorised for access at an access system (3.1, 3.2, 3.n) of another rubbish receptacle (2.1, 2.2, 2.n) which is arranged geographically at a predefined distance from the respective rubbish receptacle (2.1, 2.2, 2.n),
 - the frequency of the last use of a key (6, 6.1, 6.2, 6.n) not authorised for access at an access system (3.1, 3.2, 3.n) of another rubbish receptacle (2.1, 2.2, 2.n) arranged geographically at a predefined distance from the respective rubbish receptacle (2.1, 2.2, 2.n),
 - the value of an outstanding invoice amount owed by the user associated with this key (6, 6.1, 6.2, 6.n), and
 - the geographic distribution of the use of a key (6, 6.1, 6.2, 6.n) not authorised for access at an access system (3.1, 3.2, 3.n) of other rubbish receptacles (2.1, 2.2, 2.n).

10. The method according to claim 8 or 9,

characterised in that

if a defined number of unsuccessful access attempts of a key (6, 6.1, 6.2, 6.n) not authorised for use is exceeded, the key (6, 6.1, 6.2, 6.n) is excluded by the access system (3.1, 3.2, 3.n) from further use.

5

11. The method according to claim 10,

characterised in that

the access system (3.1, 3.2, 3.n) confiscates the key (6, 6.1, 6.2, 6.n) or deletes, overwrites or otherwise makes unusable an identification number stored on the key (6, 6.1, 6.2, 6.n).

10

12. The method according to any of claims 8 to 11,

characterised in that

the data processing by means of the data management system (1) is performed at a location separately from the respective rubbish receptacle (2.1, 2.2, 2.n).

15

13. The method according to claim 12,

characterised in that

data are transmitted between an access system (3.1, 3.2, 3.n) of a rubbish receptacle (2.1, 2.2, 2.n) and the data management system (1) wirelessly.

20

25

14. The method according to claim 12 or 13,

characterised in that

data are transmitted between an access system (3.1, 3.2, 3.n) of a rubbish receptacle (2.1, 2.2, 2.n) and the data management system (1) by means of a mobile communication connection which is preferably selected from a group consisting of a GSM connection, a UMTS connection, a GPRS connection, and an LTE connection.

30

35

15. The method according to any of claims 8 to 14,

characterised in that

steps b, e, f and g are repeated periodically, wherein the repetition occurs preferably within an interval selected from a group comprising daily, weekly, monthly, quarterly, half-yearly, or yearly repetition.

40

Revendications

45

1. Système de gestion de liste noire électronique pour un contrôle d'autorisation pour l'utilisation d'un récipient à déchets (2.1, 2.2, 2.n), le système de gestion de liste noire comportant un système de gestion de données (1) et une pluralité de systèmes d'accès (3.1, 3.2, 3.n), activables au moyen d'une pluralité de clés (6) qui sont chacune attribuables à un utilisateur ou à un groupe d'utilisateurs, pour un contrôle d'autorisation électronique pour l'utilisation d'un récipient à déchets individuel (2.1, 2.2, 2.n) attribué à chaque système d'accès individuel (3.1, 3.2, 3.n), où non seulement le système de gestion de données (1) mais encore chacun des systèmes d'accès (3.1,

50

55

3.2, 3.n) présentent une interface de communication (10.1, 10.2, 10.n) au moyen de laquelle des données sont échangeables entre le système de gestion de données (1) et chaque système d'accès individuel (3.1, 3.2, 3.n), où chaque système d'accès (3.1, 3.2, 3.n) présente un dispositif de mémoire (8.1, 8.2, 8.n) pour créer et stocker une liste des clés (6, 6.1, 6.2, 6.n) utilisées sur ce système d'accès (3.1, 3.2, 3.n) dans une période de temps déterminée, et des moyens pour transférer cette liste au système de gestion de données (1) au moyen de l'interface de communication (10.1, 10.2, 10.n), et le système de gestion de données (1) présente des dispositifs pour créer une liste noire pour le système d'accès (3.1, 3.2, 3.n) d'un récipient à déchets (2.1, 2.2, 2. n), où

- le système de gestion de données (1) est agencé pour faire appel, lors de la création de la liste noire, à un algorithme de priorisation pour prioriser les entrées dans la liste noire, l'algorithme de priorisation tenant compte au moins également de la caractéristique de la dernière utilisation d'une clé (6, 6.1, 6.2, 6.n) sans autorisation d'accès sur le système d'accès (3.1, 3.2, 3.n) du récipient à déchets respectif (2.1, 2.2, 2.n), pour créer par le système de gestion de données (1) à chaque fois un classement de priorisation individuel de toutes les clés (6, 6.1, 6.2, 6.n) sans autorisation d'accès pour le système d'accès (3.1, 3.2, 3.n) de chaque récipient à déchets (2.1, 2.2, 2.n) défini individuel, où, par le système de gestion de données (1), les clés (6, 6.1, 6.2, 6.n) sans autorisation d'accès sont reçues en commençant par la clé (6, 6.1, 6.2, 6.n) ayant la priorisation la plus élevée en classement décroissant de la priorisation dans la liste noire individuelle du système d'accès (3.1, 3.2, 3.n) de chaque récipient à déchets (2.1, 2.2, 2.n) défini individuel, jusqu'à ce que le nombre maximal des entrées de liste noire soit atteint, et

- chaque système d'accès (3.1, 3.2, 3.n) présente un dispositif de mémoire (8.1, 8.2, 8.n) pour mémoriser la liste noire créée par le système de gestion de données (1) et transférée de celui-ci sur le système d'accès respectif (3.1, 3.2, 3.n). n) pour le récipient à déchets (2.1, 2.2, 2.n) attribué à ce système d'accès (3.1, 3.2, 3.n) et chaque système d'accès (3.1, 3.2, 3.n) comporte un dispositif de traitement de données (7.1, 7.2, 7.n) et un dispositif de commande (9.1, 9.2, 9.n) pour accorder ou refuser l'accès au récipient à déchets (2.1, 2.2, 2.n) attribué au système d'accès (3.1, 3.2, 3.n) pour un utilisateur attribué à la clé (6, 6.1, 6.2, 6.n), un refus d'accès étant une conséquence d'une comparaison réussie de la clé (6, 6.1, 6.2, 6.n) avec les entrées contenues dans la liste noire individuelle

- du système d'accès (3.1, 3.2, 3.n) de ce récipient à déchets défini (2.1, 2.2, 2.n).
2. Système de gestion de liste noire électronique selon la revendication 1, **caractérisé par le fait que** l'algorithme de priorisation comporte des règles de calcul qui représentent au moins une caractéristique qui est choisie dans un groupe consistant en :
 - la fréquence de l'utilisation d'une clé (6, 6.1, 6.2, 6.n) sans autorisation d'accès sur le système d'accès (3.1, 3.2, 3.n) du récipient à déchets respectif (2.1, 2.2, 2.n) ;
 - la dernière utilisation d'une clé sans autorisation d'accès (6, 6.1, 6.2, 6.n) sur un système d'accès (3.1, 3.2, 3.n) d'un autre récipient à déchets (2.1, 2.2, 2.n), lequel est situé géographiquement à une distance prédéfinie du récipient à déchets respectif (2.1, 2.2, 2.n) ;
 - la fréquence de la dernière utilisation d'une clé sans autorisation d'accès (6, 6.1, 6.2, 6.n) sur un système d'accès (3.1, 3.2, 3.n) d'un autre récipient à déchets (2.1, 2.2, 2.n), lequel est situé géographiquement à une distance prédéfinie du récipient à déchets respectif (2.1, 2.2, 2.n) ;
 - le montant d'une facture impayée de l'utilisateur attribué à cette clé (6, 6.1, 6.2, 6.n) ; et
 - la répartition géographique de l'utilisation d'une clé sans autorisation d'accès (6, 6.1, 6.2, 6.n) sur un système d'accès (3.1, 3.2, 3.n) d'autres récipients à déchets (2.1, 2.2, 2.n).
 3. Système de gestion de liste noire électronique selon l'une des revendications 1 ou 2, **caractérisé par le fait qu'** au moins l'un des systèmes d'accès (3.1, 3.2, 3.n), de préférence une pluralité de systèmes d'accès (3.1, 3.2, 3.n), de façon davantage préférée tous les systèmes d'accès (3.1, 3.2, 3.n), présentent un dispositif pour exclure une clé (6, 6.1, 6.2, 6.n) à tous les systèmes d'accès (3.1, 3.2, 3.n) du système de gestion de liste noire électronique.
 4. Système de gestion de liste noire électronique selon la revendication 3, **caractérisé par le fait que** le dispositif pour exclure une clé (6, 6.1, 6.2, 6.n) à tous les systèmes d'accès (3.1, 3.2, 3.n) du système de gestion de liste noire électronique est un dispositif permettant de retirer la clé (6, 6.1, 6.2, 6.n) ou d'effacer, d'écraser ou de rendre inutilisable d'une autre manière un numéro d'identification mémorisé sur la clé (6, 6.1, 6.2, 6.n).
 5. Système de gestion de liste noire électronique selon l'une des revendications précédentes, **caractérisé par le fait que** l'interface de communication (10.1, 10.2, 10.n) pour l'échange des données entre le système de gestion de données (1) et chaque système d'accès individuel (3.1, 3.2, 3.n) est une interface de communication (10.1, 10.2, 10.n) appropriée pour la communication sans fil, laquelle est de préférence un dispositif de radiocommunication mobile, lequel est en particulier de préférence choisi dans un groupe consistant en un dispositif de radiocommunication mobile GSM, UMTS, GPRS et LTE.
 6. Système de gestion de liste noire électronique selon l'une des revendications précédentes, **caractérisé par le fait qu'** un système d'accès présente un dispositif de sas (4.1, 4.2, 4.n) ayant un dispositif de verrouillage (5.1, 5.2, 5.n), le dispositif de commande (9.1, 9.2, 9.n) délivrant un signal de libération pour déverrouiller le dispositif de verrouillage (5.1, 5.2, 5.n) si la comparaison de la clé (6, 6.1, 6.2, 6.n) avec les entrées contenues dans la liste noire dans le dispositif de traitement de données (7.1, 7.2, 7.n) est négative.
 7. Système de gestion de liste noire électronique selon l'une des revendications précédentes, **caractérisé par le fait qu'** un système d'accès (3.1, 3.2, 3.n) et/ou un récipient à déchets (2.1, 2.2, 2.n) présente(nt) un dispositif de localisation (11.1, 11.2, 11.n) par lequel l'emplacement actuel du récipient à déchets (2.1, 2.2, 2.n), de préférence au moyen d'un système global de navigation par satellite, en particulier de préférence choisi dans un groupe qui comporte NAVSTAR GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo et Beidou, est déterminable, la localisation étant transférable au système de gestion de données (1), de préférence par l'interface de communication (10.1, 10.2, 10.n).
 8. Procédé de gestion des données d'une liste noire dans un système d'accès pour un contrôle d'autorisation électronique pour l'utilisation d'un récipient à déchets (2.1, 2.2, 2.n), avec les étapes :
 - a. détermination d'un nombre maximal d'entrées de liste noire ;
 - b. transfert à un système de gestion de données (1) des clés (6, 6.1, 6.2, 6.n) utilisées jusqu'ici dans une période de temps déterminée sur le système d'accès (3.1, 3.2, 3.n) de chaque récipient à déchets individuel (2.1, 2.2, 2.n) d'une pluralité de récipients à déchets (2.1, 2.2, 2.n) ;
 - c. dans la mesure où le nombre maximal des entrées de liste noire n'est pas encore atteint : réception des clés (6, 6.1, 6.2, 6.n) sans autorisation d'accès dans la liste noire et transfert de la liste noire sur les systèmes d'accès (3.1, 3.2, 3.n) de tous les récipients à déchets (2.1, 2.2,

- 2.n) par le système de gestion de données (1), ou si le nombre maximal d'entrées de liste noire est atteint :
- d. détermination d'un algorithme de priorisation pour prioriser des entrées dans une liste noire pour le système d'accès (3.1, 3.2, 3.n) d'un récipient à déchets (2.1, 2.2, 2.n), l'algorithme de priorisation tenant compte au moins également de la caractéristique de la dernière utilisation d'une clé (6, 6.1, 6.2, 6.n) sans autorisation d'accès sur le système d'accès du récipient à déchets respectif (2.1, 2.2, 2.n) ;
- e. création à chaque fois d'un classement de priorisation individuelle de toutes les clés sans autorisation d'accès (6, 6.1, 6.2, 6.n) pour le système d'accès (3.1, 3.2, 3.n) de chaque récipient à déchets (2.1, 2.2, 2.n) défini individuel par le système de gestion de données (1) ;
- f. enregistrement des clés sans autorisation d'accès (6, 6.1, 6.2, 6.n), en commençant par la clé (6, 6.1, 6.2, 6.n) ayant la priorisation la plus élevée, en classement décroissant de la priorisation dans la liste noire individuelle du système d'accès (3.1, 3.2, 3.n) de chaque récipient à déchets (2.1, 2.2, 2.n) défini individuel jusqu'à ce que le nombre maximal des entrées de liste noire soit atteint, par le système de gestion des données (1) ;
- g. transfert de la liste noire individuelle sur le système d'accès (3.1, 3.2, 3.n) du récipient à déchets respectif (2.1, 2.2, 2.n) ;
- h. accord ou refus de l'accès à un récipient à déchets défini, selon les clés (6, 6.1, 6.2, 6.n) déposées dans la liste noire individuelle du système d'accès (3.1, 3.2, 3.n) du récipient à déchets (2.1, 2.2, 2.n) défini respectif.
9. Procédé selon la revendication 8, **caractérisé par le fait que** l'algorithme de priorisation prend en outre en compte des caractéristiques qui sont choisies dans un groupe consistant en :
- la fréquence de l'utilisation d'une clé sans autorisation d'accès (6, 6.1, 6.2, 6.n) sur le système d'accès (3.1, 3.2, 3.n) du récipient à déchets respectif (2.1, 2.2, 2.n) ;
 - la dernière utilisation d'une clé sans autorisation d'accès (6, 6.1, 6.2, 6.n) sur un système d'accès (3.1, 3.2, 3.n) d'un autre récipient à déchets (2.1, 2.2, 2.n), lequel est situé géographiquement à une distance prédéfinie du récipient à déchets respectif (2.1, 2.2, 2.n) ;
 - la fréquence de la dernière utilisation d'une clé sans autorisation d'accès (6, 6.1, 6.2, 6.n) sur un système d'accès (3.1, 3.2, 3.n) d'un autre récipient à déchets (2.1, 2.2, 2.n), lequel est situé géographiquement à une distance prédéfinie du récipient à déchets respectif (2.1, 2.2, 2.n) ;
 - le montant d'une facture impayée de l'utilisateur attribué à cette clé (6, 6.1, 6.2, 6.n) ; et
 - la répartition géographique de l'utilisation d'une clé sans autorisation d'accès (6, 6.1, 6.2, 6.n) sur un système d'accès (3.1, 3.2, 3.n) d'autres récipients à déchets (2.1, 2.2, 2.n).
10. Procédé selon l'une des revendications 8 ou 9, **caractérisé par le fait que** lorsqu'un nombre déterminé de tentatives d'accès rejetées d'une clé (6, 6.1, 6.2, 6.n) sans autorisation d'accès est dépassé, la clé (6, 6.1, 6.2, 6.n) est exclue de l'utilisation ultérieure par le système d'accès (3.1, 3.2, 3.n).
11. Procédé selon la revendication 10, **caractérisé par le fait que** le système d'accès (3.1, 3.2, 3.n) retire la clé (6, 6.1, 6.2, 6.n) ou efface, écrase ou rend inutilisable de toute autre manière un numéro d'identification mémorisé sur la clé (6, 6.1, 6.2, 6.n).
12. Procédé selon l'une des revendications 8 à 11, **caractérisé par le fait que** le traitement de données par le système de gestion de données (1) est effectué localement, séparément du récipient à déchets respectif (2.1, 2.2, 2.n).
13. Procédé selon la revendication 12, **caractérisé par le fait que** le transfert de données entre un système d'accès (3.1, 3.2, 3.n) d'un récipient à déchets (2.1, 2.2, 2.n) et le système de gestion de données (1) est effectué sans fil.
14. Procédé selon l'une des revendications 12 ou 13, **caractérisé par le fait que** le transfert de données entre un système d'accès (3.1, 3.2, 3.n) d'un récipient à déchets (2.1, 2.2, 2.n) et le système de gestion de données (1) est effectué au moyen d'une liaison radio mobile, laquelle est de préférence choisie dans un groupe consistant en une liaison GSM, une liaison UMTS, une liaison GPRS et une liaison LTE.
15. Procédé selon l'une des revendications 8 à 14, **caractérisé par le fait que** les étapes b, e, f et g sont réalisées de manière à se répéter périodiquement, la répétition étant de préférence réalisée dans un intervalle, lequel est choisi dans un groupe qui comporte une répétition quotidienne, hebdomadaire, mensuelle, trimestrielle, semestrielle ou annuelle.

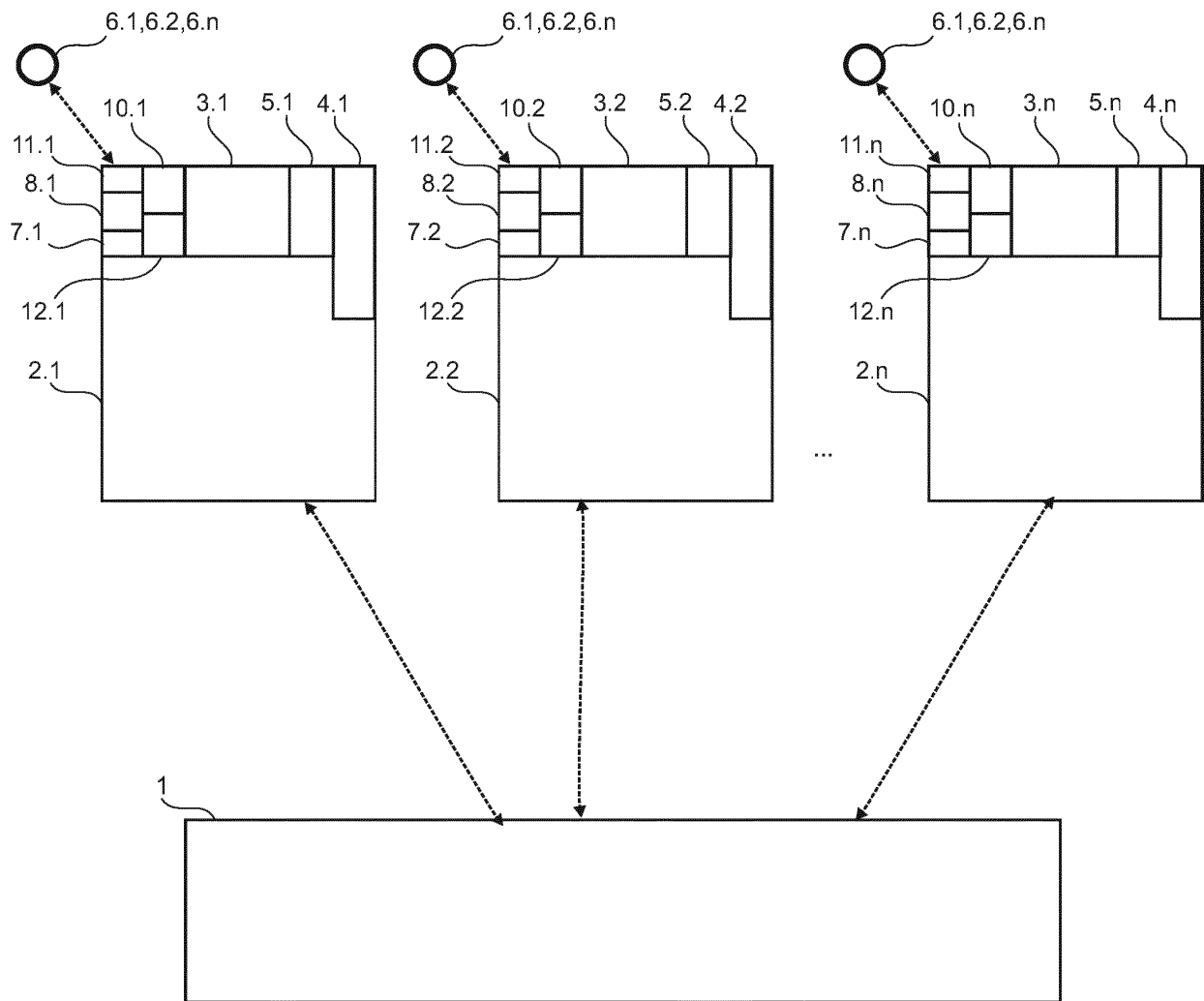


Fig. 1

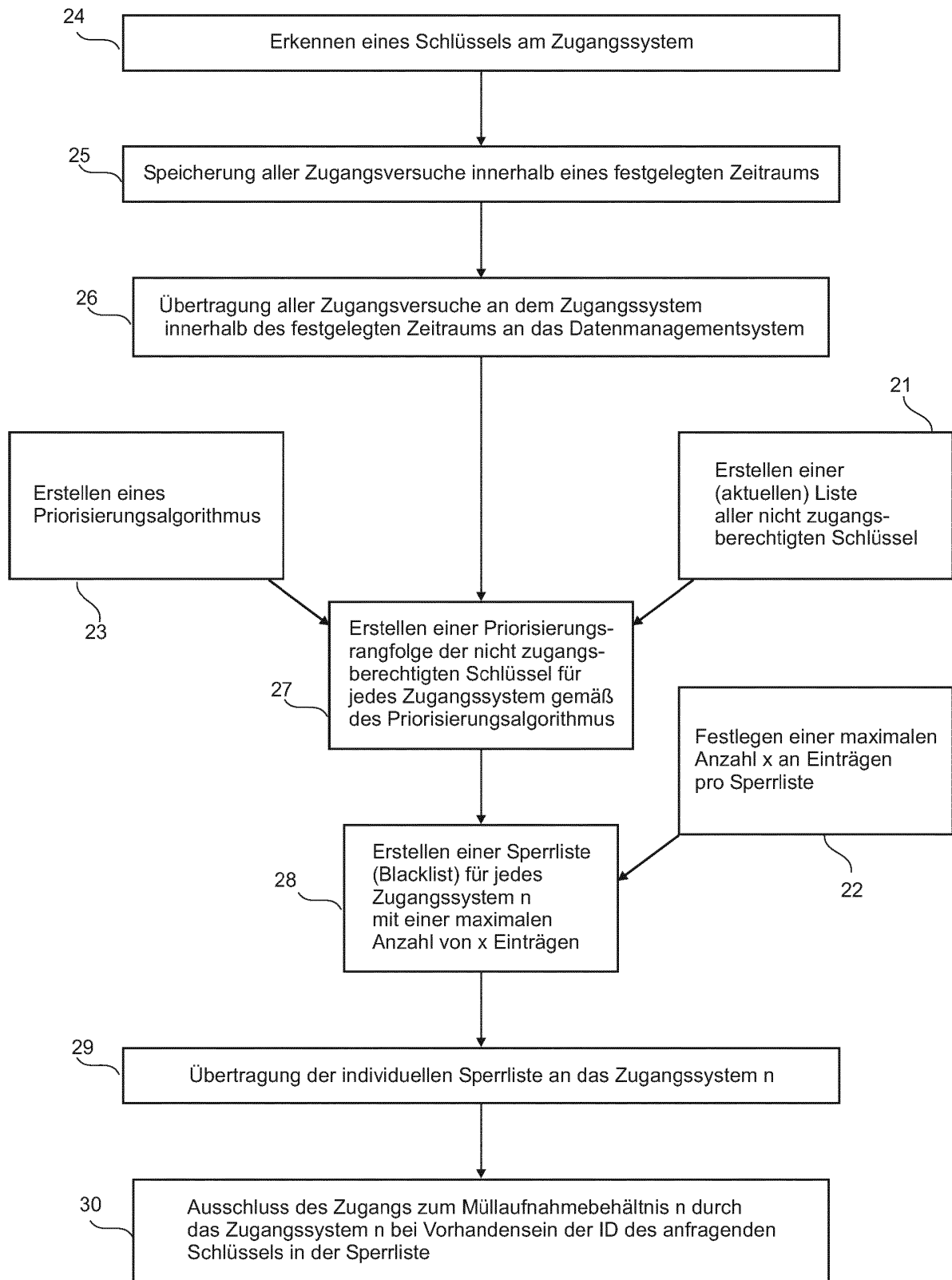


Fig. 2

Liste der Zeitstempel des Zugangssystems XY				Berechnung der Priorisierung für unberechtigte Schlüssel				Sperrliste für Zugangssystem		
Zeitstempel	Schlüssel-ID	Zeitabschnitt	Gewichtung	A8E1AD06		5CA3DA03		Prio	Sperreintrag	Summe aus
08.09.2017 17:13:21	C7B2AE01	A	10	1 x 10	10	0 x 10	0	1*	A8E1AD06	46
08.09.2017 14:41:26	3E966B04							2	5CA3DA03	28
08.09.2017 14:14:46	A8E1AD06							3	...	...
08.09.2017 14:08:16	95C8AD06							4	...	...
08.09.2017 10:14:17	FE66BB01							5	...	...
08.09.2017 08:41:46	A9B3DA03	B	8	4 x 8	32	0 x 9	0	6	...	...
07.09.2017 20:37:08	A8E1AD06							7	...	...
07.09.2017 20:36:54	A8E1AD06							8	...	...
07.09.2017 20:34:12	A8E1AD06									
07.09.2017 12:11:37	FC94DA03									
07.09.2017 01:02:49	A8E1AD06	C	6	0 x 6	0	2 x 6	12			
06.09.2017 19:43:32	D3ECB101									
06.09.2017 16:26:38	95C8AD06									
06.09.2017 16:24:20	5CA3DA03									
06.09.2017 10:01:13	9076DF01									
06.09.2017 09:54:27	5CA3DA03	D	4	1 x 4	4	4 x 4	16			
06.09.2017 09:53:40	3969E501									
06.09.2017 08:27:02	A9B3DA03									
05.09.2017 22:29:24	647DD01									
05.09.2017 22:28:47	647DD01									
05.09.2017 19:50:58	5CA3DA03	D	4	1 x 4	4	4 x 4	16			
05.09.2017 19:50:46	5CA3DA03									
05.09.2017 19:50:33	5CA3DA03									
05.09.2017 19:50:05	5CA3DA03									
05.09.2017 17:06:51	5E055004									
05.09.2017 14:06:01	A8E1AD06	D	4	1 x 4	4	4 x 4	16			
05.09.2017 11:29:35	65F4DE01									
05.09.2017 11:16:31	5E055004									
05.09.2017 09:01:51	2DCCB903									
05.09.2017 07:20:20	B19ADA03									
04.09.2017 17:14:53	B3E0B101	D	4	1 x 4	4	4 x 4	16			
04.09.2017 16:54:34	C35FE401									
...	...									
				46		28		Summe aus Gewichtung		

Anzahl Zeitstempel pro Zeitabschnitt x Gewichtungsfaktor des Zeitabschnitts

Sperrliste für Zugangssystem			Summe aus
Prio	Sperreintrag	Gewichtung	
1*	A8E1AD06		46
2	5CA3DA03		28
3	...		...
4	...		...
5	...		...
6	...		...
7	...		...
8	...		...

*) höchste Prio aufgrund der Gewichtungssumme

exemplarische Werte für Gewichtungsfaktoren einzelner Zeitabschnitte (z.B. 1 Tag):

A: 10
B: 8
C: 6
D: 4
...

unberechtigte Schlüssel

A8E1AD06	Schlüssel wurde verloren am 31.08.2017
5CA3DA03	Schlüsselbesitzer ist am 30.08.2017 ausgezogen

weitere (überlagernde) Gewichtungsfaktoren können sein:

- Zeitstempel unberechtigter Schlüssel, die noch immer benutzt werden höher gewichtet als solche die nicht mehr verwendet werden
- unberechtigte Zeitstempel (z.B. nach Verlust des Schlüssels) werden höher gewichtet als berechtigte (also vor Verlust des Schlüssels)

Fig. 3

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- KR 20150051931 A [0005]