

Electronic blocking list management system and method for checking authorisation to use a rubbish receptacle

Description

The invention relates to an electronic blocking list management system and a method for checking authorisation to use a rubbish receptacle. The method is characterised in that it prioritises entries within an exclusion list in accordance with the likelihood of an attempt to log in, so as to more quickly prevent unauthorised users from accessing a rubbish receptacle, moreover with reduced data processing effort.

In order to dispose of domestic rubbish, large rubbish containers are often provided, which are used by a number of households. Rubbish containers of this kind for example can belong to a shared household or also a community. Generally, only registered users should have access to rubbish containers of this kind, wherein the access can be blocked, for example if disposal costs are unpaid. Access of this kind can be realised by means of a wide range of different electronic systems. For example, it is known from the prior art for a user to be assigned an identification code. This identification code is stored for example on a chip or a card, which the user places into or on (for example with use of radio transmission technology for the identification code (for example by means of RFID)) a compatible reader in order to identify himself. The corresponding authentication process is performed either by a local control unit in the rubbish container or via a central server, which is connected to the local control unit of the rubbish container. Following successful authentication and assignment of the identification code to the group authorised for access, the rubbish container is then temporarily opened and the user can dispose of his rubbish.

In electronic access systems in which (writable) keys with unique ID are used (for example transponder with RFID chips), it can be necessary to block an individual one of these keys or a plurality of these keys. The need arises for example if a key is lost and measures must be taken to prevent it from still being used at the access system by unauthorised individuals. Whereas it is advantageous for electronic access systems to which only a few users are to have access (for

example a residual rubbish bin for a detached or semi-detached house) to identify only this group of residents as being authorised for access by means of a list of allowed identification codes ("whitelist"), the management of lists containing a very large number of entries of allowed identification codes, for example for central waste glass, waste clothing, or green waste containers, to which all inhabitants of a town for example have access, would signify a high data processing effort. If a very large number of keys exist for one access system, a very large number of identification codes can be necessary, which have to be stored in each access system. This has a number of disadvantages, in particular a) a large memory requirement is necessary for the identification codes, b) a high data volume arises when transmitting the large identification code lists, c) frequent updates of the identification code lists of all access systems in an area are necessary, and d) long search times can arise with large identification code lists, thus resulting in longer waiting times for the users due to the identification process before access authorisation is potentially granted. For systems of this kind it is therefore expedient to replace the list of identification codes authorised for access by a comparatively short list of identification codes for which access to the disposal system is forbidden ("blacklist").

For a blacklist of this kind, a list containing the locked entries (locked identification codes) must be stored in the memory region of the access system and is searched at the time of authentication of a key. However, in some of the above-mentioned cases, in which for example practically all inhabitants of a town have access to the disposal system, these blacklists could also become very long within a short space of time for various reasons, such that here as well the disadvantages discussed above in respect of the whitelist could also occur.

A large number of locked identification codes also have to be communicated to an access system of this kind and stored in the blacklist within a short period of time, for example due to people moving out of the area, non-payment of fees, or loss of keys or cards. In this case as well the result is that a) a large memory requirement is necessary for the locked entries, b) a high data volume arises when transmitting the large blocking lists, c) frequent updates of the blocking lists of all access systems in an area are necessary, and d) long search times can arise with large blocking lists. The blocking lists (blacklists) for access systems are generally generated by the local disposal services by means of a suitable data management system.

The object of the present invention is therefore to provide a system and a method for data management which enables effective and in particular quicker processing of a blocking list for electronic checking of authorisation to use a rubbish receptacle.

This object is achieved by an electronic blocking list management system for checking authorisation to use a rubbish receptacle according to claim 1 and by a method for data

management in a blocking list in an access system for electronic checking of authorisation to use a rubbish receptacle according to claim 8.

In terms of the apparatus, it is thus provided that the electronic blocking list management system for checking access to use a rubbish receptacle comprises a data management system and multiple access systems for electronic checking of authorisation to use an individual rubbish receptacle associated with any individual access system. The access systems can be activated by means of multiple keys, which can be allocated in each case to a user or a group of users. Both the data management system and each of the access systems has a communication interface, by means of which data can be exchanged between the data management system and each individual access system. Furthermore, each access system has a memory device for creating and storing a list of the keys used at this access system within a defined period of time and means for transmitting this list by means of the communication interface to the data management system. An access system of this kind preferably also has a time-tracking device, such that a timestamp can be added to each access attempt by means of the key. The timestamp is preferably stored with the corresponding entry of the access attempt of the key used at this access system. It is in particular preferred that the timestamp is transmitted to the data management system together with the corresponding entry of the access attempt of the key used at this access system. The data management system, which preferably has a larger memory capacity and has a greater computing power than the access system, can thus archive the data regarding access attempts with certain keys together with the timestamp. The usefulness of the data regarding access attempts ascertained by the access system is thus insured over a long period of time.

The data management system has devices for creating a blocking list for the access system of a rubbish receptacle, wherein the data management system, when creating the blocking list, can refer back to a prioritisation algorithm for prioritising entries in the blocking list. The prioritisation algorithm here also takes into consideration at least the feature of the last use of a key not accessed for authorisation at the access system of the respective rubbish receptacle. Due to the use of the feature of the last use of a key not authorised for access at the access system of the respective rubbish receptacle, it is possible to prevent keys which have been destroyed or lost and remain unfound from still having to be included in the blocking list and blocking a memory space. If a lost key is found again, it would thus be possible to use said key again (if it were no longer contained in the blocking list due to the long period of non-use), since said key would not be on the blocking list, however it would be added to the blocking list again at the time of the next update due to the renewed use and would be listed with correspondingly high priority on the blocking list on account of the recent use.

Each access system additionally has a memory device for storing the blocking list created by the data management system and transmitted therefrom to the respective access system for the

rubbish receptacle associated with said access system. The blocking list is therefore available to this access system also after the data transmission for comparison with keys requesting use of the associated rubbish receptacle. An existing data connection with the data management system is therefore unnecessary. In addition, each access system comprises a data processing device and a control device for granting or refusing access to the rubbish receptacle associated with the access system for a user associated with the key, wherein access refusal results from a successful comparison of the key with the entries contained in the blocking list. The data processing device compares a key requesting use of the rubbish receptacle associated with the access system with the entries contained in the blocking list. If the key is not excluded from use of the rubbish receptacle associated with the access system, access to the rubbish receptacle can be granted by the control device.

Precisely one rubbish receptacle is preferably associated with each access system. An access system can thus monitor the access to the rubbish receptacle associated therewith.

The authorisation to use a rubbish receptacle is checked by means of keys. Each user or group of users is assigned a key. A key of this kind can be for example an identification number (ID). It is noted in this regard that the term "identification number" is not limited to numbers, and instead is used generally for any sequence of symbols enabling association with a user. This ID can be for example a PIN (personal identification number (PIN code)) to be input by the user or can be stored on a data carrier readable by the access system. A readable data carrier of this kind is preferably a data carrier selected from a group comprising a chip card, an RFID tag, a mobile telephone, a tablet, laptop, a finger (fingerprint), the face (facial scan) and an eye (iris scan). Due to the lower equipment requirements and lower energy consumption, in particular a chip card, RFID tag or a mobile telephone (for example via NFC (near field communication) or Bluetooth) are preferred for identifying a user. The NFC technology is particularly preferred, since in the meantime practically all smartphones support this technology and there is thus a very wide prevalence of appropriate identification devices.

In order to monitor and control access to the rubbish receptacle, an access system usually requires energy, generally electricity. Since the rubbish receptacles are often located in public areas, in many cases there is no access to a mains supply. A decentralised energy supply is therefore preferred. This could be provided for example by primary cell or secondary batteries, or solar power. Combinations of these or supplementations with other energy sources are also possible. For example, it is conceivable that the required energy is obtained by solar energy and is stored in secondary batteries. A primary battery as emergency power source, if there are no other energy sources available, is also conceivable (independently and in combination with other energy sources).

Since, as mentioned above, access to the mains grid is often unavailable in systems of this kind, the use of energy-intensive data-processing systems is possible only to a very limited extent with regard to the control and monitoring of the access to the rubbish receptacle. The associated restrictions with regard to the performance of the data processing systems lead to the aforementioned delay when checking access authorisations from a list containing a very large number of entries. In order to avoid or at least reduce delays of this kind, it is necessary to define a maximum number of entries in a list from which the access authorisation is ascertained. In particular in systems with a very large number of individuals authorised for access, the option of a whitelist is therefore eliminated (as described at the outset). Systems with a very high number of individuals authorised for access can be managed particularly efficiently by means of a blacklist or blocking list entries. Since lists containing blocking list entries can also exceed a critical size over time, a maximum number of blocking list entries must also be defined for these lists, so as to be able to ensure quick processing by the access system.

It is preferably provided that an access system has a port device with a locking device. The port device can be used for example to throw rubbish into the rubbish receptacle. Only if a locking device is unlocked can a port access point be opened by the user (or also the access system itself). In a preferred embodiment, the control device emits a release signal in order to unlock the locking device. However, this is implemented only if the comparison of the key with the entries contained in the blocking list is negative in the data processing device.

On account of the frequent arrangement of rubbish receptacles in freely accessible public spaces, access to a wired data network is often also absent or very limited. In a preferred embodiment, the communication interface for exchanging data between the data management system and each individual access system is therefore preferably a communication interface suitable for wireless communication. On account of the large network coverage, a mobile communication device is preferred here in particular, and particularly preferably selected from a group comprising a GSM, UMTS, GPRS and LTE mobile communication device. Alternatively or additionally, a WLAN connection (connection via a wireless local network (Wireless Local Area Network)) is also conceivable, since in the meantime, networks of this kind have also become available in many towns. Alternatively to wireless data transmission, transmission by means of a data carrier (for example a memory card or a memory stick (for example USB stick)) is also possible. This could be implemented for example at the time of or during the emptying of the rubbish receptacle. Since the data transmission often is not time-critical and for example can be performed overnight or during times of low use of the transmission network, the speed of the data transmission is of secondary importance, in particular in the case of wireless data transmission.

In a further preferred embodiment, an access system and/or a rubbish receptacle has a locating device, by means of which the current location of the rubbish receptacle can be determined. The

locating device more preferably uses a global navigation satellite system in order to determine the current location. This is selected particularly preferably from a group comprising NAVSTAR GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo and Beidou. The current location preferably can be transmitted to the data management system, preferably via the communication interface already mentioned above. The determination and transmission of the current location of the rubbish receptacle to the data management system has the advantage that a rubbish receptacle distanced from the intended location, for example due to vandalism or theft, can be easily located. In addition, the further rubbish receptacles located in the vicinity of this rubbish receptacle can also be determined, and this can be taken into consideration for the determination of the blocking list, as will be presented further below.

The prioritisation algorithm is of particular importance for efficient assignment of individual keys to the blocking lists of individual rubbish receptacles or the respective access system associated with this rubbish receptacle. A blocking list which on the one hand is as short as possible, but on the other hand contains so many blocking entries that unauthorised use of the respective rubbish receptacle is prevented or at least minimised with high likelihood preferably can be generated by use of this prioritisation algorithm.

In a preferred embodiment the prioritisation algorithm comprises computing specifications which display at least one feature selected from the group comprising

- the frequency of use of a key not authorised for access at the access system of the respective rubbish receptacle,
- the last use of a key not authorised for access at an access system of another rubbish receptacle which is arranged geographically at a predefined distance from the respective rubbish receptacle,
- the frequency of the last use of a key not authorised for access at an access system of another rubbish receptacle arranged geographically at a predefined distance from the respective rubbish receptacle,
- the value of an outstanding invoice amount owed by the user associated with this key, and
- the geographic distribution of the use of a key not authorised for access at an access system of other rubbish receptacles.

By displaying one or more of these features in the computing specifications of the prioritisation algorithm, various conceivable scenarios of the misuse of a key can be predicted, and the respective access systems of the respective rubbish receptacles can be prepared for the likely misuse of a key by inclusion thereof in the respective blocking list.

If, for example, the frequency of use of a key not authorised for access at an access system of a specific rubbish receptacle is very high, it is very likely that the user (now) no longer authorised for use is still highly likely attempting to use this rubbish receptacle. The misuse can be prevented by a correspondingly high prioritisation of this key in the blocking list created individually for this rubbish receptacle.

It is also highly likely that a user not authorised (any more) for access will attempt to use rubbish receptacles in the vicinity of a previously preferred and often-used rubbish receptacle. Since (as mentioned above) the (current) position of the individual rubbish receptacles is known, monitored or determined as required, rubbish receptacles which are arranged geographically at a predefined distance from the rubbish receptacle last used by the user who is to be barred can thus be quickly determined. If the last use of a key not authorised for access at an access system of another rubbish receptacle arranged geographically at a predefined (short) distance from the respective rubbish receptacle was not too long ago, this can be used for a high prioritisation of this key also at a rubbish receptacle not previously used by this user.

If the frequency of the last use of a key not authorised for access at an access system of another rubbish receptacle arranged geographically at a predefined (short) distance from the respective rubbish receptacle is very high, this can also indicate that the unauthorised user is frequently active in this area and could highly likely also use this rubbish receptacle in the future. A high prioritisation of this key at this rubbish receptacle as well also leads to a refusal of use, even before the first use attempt.

It is also conceivable to base the prioritisation on the geographical distribution of the use of a key (now) not authorised for use (any more) at an access system of other rubbish receptacles. If a user for example previously used predominantly two different rubbish receptacles (for example at home and at the workplace), rubbish receptacles arranged geographically therebetween (for example in the region of main roads) could be excluded from use to this user on the basis of a consideration of the geographical distribution, by including these rubbish receptacles with correspondingly high prioritisation in the respective blocking lists of the access system of the rubbish receptacles positioned there.

A further possible criterion for high prioritisation could be the value of an outstanding amount invoiced to the user associated with this key. By means of a high prioritisation of this kind, users who do not pay bills over a long period of time can also be denied use of rubbish receptacles which are distanced very far from the rubbish receptacles usually used and on the blocking list of which this defaulting user on the basis of the criteria presented above otherwise would not be included on account of the large distance.

In a preferred embodiment the electronic blocking list management system is characterised in that at least one of the access systems, preferably multiple access systems, more preferably all access systems, has/have a device for excluding a key with respect to all access systems of the electronic blocking list management system. A device of this kind for excluding a key with respect to all access systems of the electronic blocking list management system could, in a preferred embodiment, for example be an apparatus for confiscating the key or for deleting, overwriting or otherwise making unusable an identification number stored on the key.

If chip cards are used for example for identification, these could be withheld by the access system following (possibly multiple) unauthorised or unsuccessful access attempts. When the rubbish receptacle is emptied, the withheld chip card could be removed from the access system by operating staff and thus taken out of circulation.

In the case of identification via a key which does not have to be brought physically into contact with the access system (for example an RFID tag, a mobile telephone or another system working contactlessly), the withholding option is usually not possible, and therefore the key must be made unusable by deletion, overwriting, or in some other way. For example, it would be conceivable that all keys within an area contain a uniform prefix which classifies them as belonging to this area (for example a town, a suburb, a place, or a district). If this prefix is deleted, overwritten or made unusable in another way, the access systems in this area will no longer respond to this key, and therefore use of this key will be excluded for the entire area.

If an access system during the authentication process identifies the ID of an unauthorised key, the access system can thus selectively destroy the data of the unauthorised key by means of write access or at least change it in such a way that the function of the key is interrupted. The authentication process for the unauthorised key will therefore no longer function at any other access system either.

In this regard, it is particularly preferred if the information of a destroyed key is transmitted from the destroying access system to the data management system. The locked entry of this key can thus be deleted from all blocking lists, whereby free space can be created for a further unauthorised key.

In terms of the method, the object addressed by the invention is achieved by a method for data management of a blocking list in an access system for electronically checking authorisation to use a rubbish receptacle, said method being characterised by the following steps

- a. defining a maximum number of blocking list entries,

- b. transmitting to a data management system the key used previously within a defined period of time at the access system of any individual rubbish receptacle from multiple rubbish receptacle containers,
- c. including the key not authorised for access in the blocking list until the maximum number of blocking list entries is reached, and transmitting the blocking list to the access systems of all rubbish receptacles by means of the data management 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 of a rubbish receptacle, wherein the prioritisation algorithm at least also takes into consideration the feature of the last use of a key not authorised for access at the access system of the respective rubbish receptacle,
- e. creating, by the data management system, an individual prioritisation hierarchy for all keys not authorised for access for the access system of each individual defined rubbish receptacle,
- f. including, by means of the data management system, the keys not authorised for access, starting with the key with the highest prioritisation in descending hierarchy of the prioritisation, in the individual blocking list of the access system of each individual defined rubbish receptacle until the maximum number of blocking list entries is reached,
- g. transmitting the individual blocking list to the access system of each individual defined rubbish receptacle, and
- h. granting or refusing access to a defined rubbish receptacle in accordance with the keys stored in the individual blocking list of the access system of the respective defined rubbish receptacle.

A maximum number of the blocking list entries is defined, as already presented above, preferably depending on the performance of the respective access system. Since a small number of blocking list entries enables relatively quick data processing, even in the case of relatively inefficient access systems, a small maximum number of blocking list entries is preferred. The maximum number of blocking list entries is particularly preferably 5000 entries, more preferably 2^{12} entries, more preferably 2^{11} entries, particularly preferably 2^{10} entries, more preferably 1000 entries, more preferably 2^5 entries, more preferably 500 entries, particularly preferably 400 entries, more preferably 2^8 entries, more preferably 2^7 entries, and particularly preferably 100 entries. With such a small number of entries, a comparison can be made with a blocking list by the access system practically without any noticeable delay for the user using current hardware, moreover with an extremely low power consumption. A maximum number of the blocking list entries does not have to be redefined each time a blocking list is updated. The retention of a previously defined value of a maximum number of blocking list entries is therefore also understood as the defining of a maximum number of blocking list entries within the sense of this invention.

As presented above, the last (and/or frequent) use of a key at a rubbish receptacle or at a rubbish receptacle in the geographic vicinity is of significance for the assessment of the likelihood of misuse of a rubbish receptacle. It is therefore provided that the keys used previously within a defined period of time at the access system of any individual rubbish receptacle from multiple rubbish receptacles are transmitted (preferably repeatedly at regular intervals) to a data management system.

If the maximum number of blocking list entries has not yet been reached, all keys not authorised for access can be included in the blocking list. This blocking list is the same for the access systems of all rubbish receptacles, and therefore can be transmitted to all access systems by the data management system. However, at the latest when the maximum number of blocking list entries is reached, it is provided that a prioritisation algorithm is defined for prioritising entries in a blocking list for the access system of a rubbish receptacle. Here, the prioritisation algorithm takes into consideration at least also the feature of the last use of a key not authorised for access at the access system of the respective rubbish receptacle. Since any access attempt at individual rubbish receptacles is thus taken into consideration when creating the blocking lists, individual blocking lists are necessary. Each rubbish receptacle is therefore assigned an individual blocking list which at least in good approximation reflects the likelihood for misuse of a key at precisely this rubbish receptacle.

An individual prioritisation hierarchy of all keys not authorised for access is thus created for the access system of each individual defined rubbish receptacle by means of the data management system. Based on this prioritisation hierarchy, starting with the key with the highest prioritisation in decreasing hierarchy of prioritisation, an individual blocking list is now generated for the access system of each individual defined rubbish receptacle, wherein each entry is included in the individual blocking list until the maximum number of blocking list entries is reached. Alternatively, if the number of entries in accordance with the prioritisation hierarchy exceeds the maximum permissible number of blocking list entries, the entry listed in this hierarchy with the lowest prioritisation could be deleted, until the number of keys of this individual prioritisation hierarchy corresponds to the maximum permissible number of blocking list entries. Keys for which use at precisely this rubbish receptacle is unlikely are not contained in the blocking list associated with this rubbish receptacle, provided the placement thereof in the prioritisation hierarchy would exceed the maximum number of list entries.

The individual blocking lists thus generated in each case for a specific access system are then transmitted to the access system of the respective rubbish receptacle. The blocking list containing the keys most likely to be misused for this rubbish receptacle is thus available for future reference

to the access system there, even without an existing data connection, and enables an evaluation of access authorisation for a specific key.

If a user now attempts to gain access to the rubbish receptacle using a specific key, the access system can grant or refuse access in accordance with the keys stored in the individual blocking list for the respective rubbish receptacle. It is thus possible only for users whose key is not contained in the individual blocking list stored in the access system of this rubbish receptacle to use this rubbish receptacle.

The term "individual blocking list" shall be understood within the context of this invention such that a blocking list is determined separately for each rubbish receptacle or each group of rubbish receptacles. However, it is quite conceivable that the separately determined blocking lists can also be identical for various rubbish receptacles. Such identical blocking lists shall be understood to be individual blocking lists in the sense of this invention.

As already described above in respect of the apparatus, it is also advantageous in respect of the method if the prioritisation algorithm also takes into consideration features that are selected from the group comprising

- the frequency of use of a key not authorised for access at the access system of the respective rubbish receptacle,
- the last use of a key not authorised for access at an access system of another rubbish receptacle which is arranged geographically at a predefined distance from the respective rubbish receptacle,
- the frequency of the last use of a key not authorised for access at an access system of another rubbish receptacle arranged geographically at a predefined distance from the respective rubbish receptacle,
- the value of an outstanding invoice amount owed by the user associated with this key, and
- the geographic distribution of the use of a key not authorised for access at an access system of other rubbish receptacles.

If a defined number of unsuccessful access attempts of a key not authorised for access is exceeded, the key is advantageously excluded from further use by the access system. This can be achieved preferably in that the access system confiscates the key or deletes, overwrites or in some other way makes unusable an identification number stored on the key.

A method in which the data processing by the data management system is performed at a location separately from the respective rubbish receptacle is also preferred. This has the advantage that the data processing by means of the data management system can be performed centrally for all

rubbish receptacles. It is preferably performed at a location at which sufficient power is available for operation of an efficient data management system and optionally also an archiving system. Information regarding unauthorised access attempts can thus be archived over a long period of time and/or in the event of renewed use of a key which has not been used for a long period of time, the use data associated with this key can be used again.

The data can be transmitted, for example, when the rubbish receptacle in question is emptied. However, an alternative method variant in which data is transmitted wirelessly between an access system of a rubbish receptacle and the data management system is preferred. This enables data exchange also at times between two emptying processes, for example if misuse of a rubbish receptacle is anticipated soon. In the case of wireless transmission of data, it is unnecessary to send a worker to update the blocking list of a rubbish receptacle.

A method variant in which data is transmitted between an access system of a rubbish receptacle and a data management system by means of a mobile communication connection preferably selected from a group comprising a GSM connection, a UMTS connection, a GPRS connection, and an LTE connection is particularly preferred.

In a preferred method variant the above-mentioned 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. An up-to-date data state in the access systems of all rubbish receptacles can thus be ensured.

Of course, it is also conceivable to apply the described system and method for controlling the access for rubbish receptacles of various types of rubbish, for example residual waste, paper waste, bottle waste, metal waste, wood waste, green waste, hazardous waste, residual medication waste or plastic waste containers.

Further advantages, objectives and properties of the present invention will be explained on the basis of the following description of the accompanying drawings. Similar components can have the same reference signs in the various embodiments.

In the drawings:

Fig. 1 shows an overview of an electronic blocking list management system for checking authorisation to use a rubbish receptacle;

Fig. 2 shows a basic diagram of the electronic blocking list management system for checking authorisation to use a rubbish receptacle in accordance with one embodiment;

Fig. 3 shows an exemplary illustration for creating a prioritisation hierarchy and a resultant individual blocking list.

Figure 1 shows an overview of the electronic blocking list management system for checking authorisation to use a rubbish receptacle. This system comprises a data management system (1). This can be arranged centrally and is preferably physically separate from each of the rubbish receptacles (2.1, 2.2, 2.n). Each of the rubbish receptacles (2.1, 2.2, 2.n) is connected to an access system (3.1, 3.2, 3.n), which controls the access to the respective rubbish receptacle (2.1, 2.2, 2.n). To this end, a port device or transfer device (4.1, 4.2, 4.n) is provided, which can be locked by means of a locking device (5.1, 5.2, 5.n). If the port device (4.1, 4.2, 4.n) is locked, access to the respective rubbish receptacle (2.1, 2.2, 2.n) is blocked and it is not possible to dispose of rubbish in this rubbish receptacle (2.1, 2.2, 2.n).

The fact of whether a user is permitted to dispose of rubbish and whether the port device (4.1, 4.2, 4.n) can be opened by the user by unlocking of the locking device (5.1, 5.2, 5.n) is decided by the access system (3.1, 3.2, 3.n) on the basis of a key assigned to the user, for example an ID (6.1, 6.2, 6.n). To this end, the access system (3.1, 3.2, 3.n) has a data processing device (7.1, 7.2, 7.n) and a memory device (8.1, 8.2, 8.n). An individual blocking list associated with the respective rubbish receptacle (2.1, 2.2, 2.n) is stored in the respective memory device (8.1, 8.2, 8.n) and contains those keys (6.1, 6.2, 6.n) for which access to this rubbish receptacle (2.1, 2.2, 2.n) should be refused.

If, by contrast, a key (6.1, 6.2, 6.n) that is not contained in the individual blocking list of this rubbish receptacle (2.1, 2.2, 2.n) is used by the user, the locking device (5.1, 5.2, 5.n) is unlocked via a control device (9.1, 9.2, 9.n) likewise contained in the access system (3.1, 3.2, 3.n), and the access to the port device (4.1, 4.2, 4.n) is released to the user, such that said user can throw rubbish through the port device (4.1, 4.2, 4.n) into the rubbish receptacle (2.1, 2.2, 2.n).

The key (6.1, 6.2, 6.n) of the user is read in by the respective access system (3.1, 3.2, 3.n) via a communication interface (10.1, 10.2, 10.n). The key (6.1, 6.2, 6.n) can be for example a chip card, an RFID tag, or a mobile telephone. The communication interface (10.1, 10.2, 10.n) is preferably suitable for wireless communication.

In the present embodiment, the access system (3.1, 3.2, 3.n) of each rubbish receptacle (2.1, 2.2, 2.n) also has a locating device (11.1, 11.2, 11.n) and a time-tracking device (12.1, 12.2, 12.n). The current location of the respective rubbish receptacle (2.1, 2.2, 2.n) can be determined by means of the locating device (11.1, 11.2, 11.n), for example by means of NAVSTAR GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo or Beidou or a combination of

various systems. The time-tracking device (12.1, 12.2, 12.n) can be used to assign a unique timestamp to each use attempt of a user, so that each use attempt for each rubbish receptacle (2.1, 2.2, 2.n) can be documented both in terms of location and in terms of time. In addition or alternatively, the location determination of the access system could also be performed on-site at the time of commissioning or maintenance by means of a service tool (for example smartphone app), which can detect GPS data and stores the location data of the access system or of the rubbish container either directly in the data management system or in the access system. The access system can then transmit this data via radio to the data management system.

The communication interface (10.1, 10.2, 10.n) is also used for data transmission to and from the data management system (1). To this end, the communication interface (10.1, 10.2, 10.n) preferably has a separate communication channel. This differs preferably from that by means of which the key of a user is read. The two communication channels of the communication interface (10.1, 10.2, 10.n) can also be embodied as separate subunits which are arranged spatially distanced from one another in or on the rubbish receptacle (2.1, 2.2, 2.n) and/or the access system (3.1, 3.2, 3.n).

The communication interface (10.1, 10.2, 10.n) is preferably designed for wireless communication with the data management system (1). This has the advantage that the data do not have to be exchanged by hand (for example by means of a USB stick) by operating staff. A mobile communication connection is preferably used for data exchange between the communication interface (10.1, 10.2, 10.n) and the data management system (1).

Figure 2 shows a basic diagram of the electronic blocking list management system for checking authorisation to use a rubbish receptacle in accordance with one embodiment. As is shown in this basic diagram, a list of all keys not authorised for access is created in a step (21). If this list is so long that delayed authentication of keys at the access system (3.1, 3.2, 3.n) of the respective rubbish receptacle (2.1, 2.2, 2.n) is anticipated, a maximum number x of entries per blocking list (blacklist) is defined in step 22. If this number x is lower than the number of all entries in the list of keys not authorised for access, it is necessary in step (23) to define criteria by means of which a prioritisation algorithm can define a prioritisation hierarchy of keys not authorised for access.

To enable effective access control to a specific rubbish receptacle (for example 2.1 from multiple rubbish receptacles (2.1, 2.2, 2.n)), all access attempts of all keys at each access system (3.1, 3.2, 3.n) of the system are first identified in step (24), and in step (25) are stored for a defined period of time in the memory device of the access system (3.1, 3.2, 3.n).

In step (26), the data regarding access attempts stored in one or more access systems (3.1, 3.2, 3.n) are transmitted to the data management system (1). This transmission can be performed at

regular intervals, initiated by the user, or when a predefined memory usage of the memory device (8.1, 8.2, 8.n) of the respective access system (3.1, 3.2, 3.n) is exceeded (for example > 75 %, preferably > 80 %, particularly preferably > 90 %). Following the transmission, the transmitted data can be stored and archived in the data management system (1), such that the memory device (8.1, 8.2, 8.n) of the respective access system (3.1, 3.2, 3.n) can be emptied for the storage of new data relating to access attempts.

If the data relating to access attempts are transmitted to the data management system (1), a prioritisation hierarchy for the keys not authorised for access can be created there in step (27) for each access system (3.1, 3.2, 3.n) on the basis of the previously defined prioritisation algorithm (see step 23). Since the data relating to access attempts at the various rubbish receptacles (2.1, 2.2, 2.n) differs, there is an individual prioritisation hierarchy for each rubbish receptacle (2.1, 2.2, 2.n) on the basis of the access attempts and the underlying prioritisation algorithm. In particular in larger systems having a very large number of rubbish receptacles (2.1, 2.2, 2.n), a relatively high computing effort is therefore anticipated.

Based on the individual prioritisation hierarchy, an individual blocking list (blacklist) is produced in step (28) for each rubbish receptacle (2.1, 2.2, 2.n). This is limited to a number of x entries in order to keep the data processing by the access system (3.1, 3.2, 3.n) on-site as low as possible. Entries for which the position in the prioritisation hierarchy exceeds the number x are not included in the blocking list.

Following the generation of the blocking lists, in step (29) the individual blocking list is transmitted to the respective access system (3.1, 3.2, 3.n). Depending on the available bandwidth of the transmission network, this can be performed jointly at the same time for all blocking lists and access systems (3.1, 3.2, 3.n) or merely for individual access systems (3.1, 3.2, 3.n) or a group of access systems (3.1, 3.2, 3.n).

Following the transmission, the respective blocking list is available in the corresponding access system (3.1, 3.2, 3.n) for assessment of the access authorisation for users of a specific key. If the key with which a user is requesting access to the rubbish receptacle (2.1, 2.2, 2.n) is contained in the blocking list of the access system (3.1, 3.2, 3.n) of this rubbish receptacle (2.1, 2.2, 2.n), the access to the rubbish receptacle (2.1, 2.2, 2.n) is refused and the locking device (5.1, 5.2, 5.n) remains locked.

Figure 3 shows an example depiction of the creation of a prioritisation hierarchy and a resultant individual blocking list. In the left-hand region (columns 1 and 2), all data relating to access attempts at a specific rubbish receptacle over a period of time of a few successive days and transmitted to the data management system (1) are shown. The respective data records contain a

timestamp and a key ID. The data records contain both access attempts of permitted keys and (in this case two) keys that are not permitted (key ID shown in bold).

Specific weighting factors (in this case 10, 8, 6 and 4) are stored in the data management system (1) for each time period (in this case A, B, C and D). In the example shown, each of the access attempts with a key that is not permitted is assigned the weighting factor associated with the respective time period. The product of the number of access attempts per time period and the respective weighting factor gives a value for each time period and each key that is not permitted. If the values for each key are summed individually, the sum gives a weighting value on the basis of which the prioritisation can be made. In the present example, on the basis of the determined sum of 46, the key A8E1AD06 is prioritised higher than the key 5CA3DA03, which merely came to a sum of 28.

The values presented here by way of example for the weighting serve merely for illustration. The weighting can be adapted to the respective requirements. In addition, the system can also be optimised by further weighting factors. For example, in the case of keys not authorised for access, the reason for withdrawal of the access authorisation can also be included in the weighting.

If, for example, a key has been lost and another key loses access authorisation due to an inhabitant moving out, a higher weighting could be advantageous for the lost key due to the unknown identity of the user and the higher likelihood of illegal use, whereas the inhabitant who has moved can still be identified and therefore any use fees of the rubbish receptacle can still be claimed.

In addition, timestamps for unauthorised keys that are still being used could for example be weighted more highly than those that are no longer being used and/or unauthorised timestamps (for example following loss of the key) could be weighted more highly than authorised timestamps (i.e. before loss of the key).

All features disclosed in the application documents are claimed as essential to the invention insofar as they are novel individually or in combination in relation to the prior art.

List of reference signs

1	data management system
2.1, 2.2, 2.n	rubbish receptacles
3.1, 3.2, 3.n	access system
4.1, 4.2, 4.n	port device
5.1, 5.2, 5.n	locking device
6.1, 6.2, 6.n	key, ID
7.1, 7.2, 7.n	data processing device
8.1, 8.2, 8.n	memory device
9.1, 9.2, 9.n	control device
10.1, 10.2, 10.n	communication interface
11.1, 11.2, 11.n	locating device
12.1, 12.2, 12.n	time-tracking device
21-30	step

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), characterised in that

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),

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), when creating the blocking list, can access a prioritisation algorithm for prioritising entries in 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),

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 blocking list,

at least one of the access systems (3.1, 3.2, 3.n), has 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.
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 comprising

- 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 a plurality of access systems (3.1, 3.2, 3.n) 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 any of the preceding claims, characterised in that all access systems (3.1, 3.2, 3.n) 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.
5. The electronic blocking list management system according to any of the preceding claims, 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).
6. 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.) is a communication interface (10.1, 10.2, 10.n) suitable for wireless communication.

7. The electronic blocking list management system according to claim 6, characterised in that the communication interface (10.1, 10.2, 10.n) is a mobile communication device.
8. The electronic blocking list management system according to claim 7, characterised in that the mobile communication device is selected from a group comprising a GSM, UMTS, GPRS and LTE mobile communication device.
9. The electronic blocking list management system according to any of the preceding claims, characterised in that each 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).
10. The electronic blocking list management system according to any of the preceding claims, characterised in that each 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, wherein the location can be transmitted to the data management system (1), via the communication interface (10.1, 10.2, 10.n).
11. The electronic blocking list management system according to claim 10, characterised in that the location of the rubbish receptacle (2.1, 2.2, 2.n) can be determined by means of a global navigation satellite system.
12. The electronic blocking list management system according to claim 11, characterised in that the global navigation satellite system is selected from the group comprising NAVSTAR GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo and Beidou.

13. 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), characterised by 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 has not yet been reached: including the key (6, 6.1, 6.2, 6.n) not authorised for access in the blocking list, 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 and carrying out step h), or
if the maximum number of blocking list entries is reached: carrying out steps d) – g),
 - 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).
14. The method according to claim 13, characterised in that

the prioritisation algorithm also takes into consideration features selected from the group comprising

- 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).

15. The method according to claim 13 or 14, 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.
16. The method according to claim 15, 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).
17. The method according to any of claims 13 to 16, 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).
18. The method according to claim 17, characterised in that
data are transmitted between the 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.

19. The method according to claim 17 or 18,
characterised in that
data are transmitted between the 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.
20. The method according to claim 19,
characterised in that
the mobile communication connection is selected from a group comprising a GSM connection, a UMTS connection, a GPRS connection, and an LTE connection.
21. The method according to any of claims 13 to 20,
characterised in that
steps b, e, f and g are repeated periodically.
22. The method according to any of claim 21,
characterised in that
the repetition occurs within an interval selected from a group comprising daily, weekly, monthly, quarterly, half-yearly, or yearly repetition.