

Method for operating an access system

Description

The invention relates to a method for operating an access system for an access device, in particular for a refuse container.

Large-scale refuse containers that are used by several households are often provided for disposing of household refuse. Such refuse containers can belong to a household or a community, for example. Such refuse containers generally comprise an access device so that authorised users gain access to such refuse containers. Authorisation can also be blocked again, for example if the disposal costs are not paid. Such access can be provided by means of a wide variety of electronic systems. It is known in the art, for example, that an identification code is assigned to a user. This identification code is entered by means of a numeric keypad arranged on the refuse container, for example. However, such systems are impractical for the user, since said user always has to have the access data at hand. Furthermore, loss of the access data involves a complex administrative process.

The previous use of PIN input fields or RFID tags and cards is also disadvantageous in that the user requires additional hardware and/or additional knowledge. Additional costs and administrative effort are required, since the hardware has to be issued or sent to the user. Furthermore, protection against misuse proves difficult, depending on the specific method. It

is difficult, if not impossible, to put a time limit on the access; in the case of key-based access, all locks would need to be replaced and all keys re-issued, for example.

The object of the present invention is to provide an improved method for operating an access system for an access device.

This object is achieved by a method for operating an access system that comprises an access device, in particular for a refuse container, comprising the following steps:

- a. registering the user using a communication apparatus of a data management system by means of a first communication channel;
- b. sending a data record to the communication apparatus by means of the data management system via the first communication channel, the data record comprising authentication data and validation data;
- c. initiating the exchange of data between the communication apparatus and the access device via a second communication channel, at least the authentication data being transferred to the access device, the second communication channel being a wireless connection;
- d. checking the authentication data for the authorisation of the user using a control means of the access device;

the registration being carried out only once and the authentication data authorising access to the access device in a predetermined validity range, the communication apparatus not having to be connected to the data management system by means of a first communication channel when data are exchanged via the second communication channel.

The user can therefore access a refuse container as conveniently as possible, access to which is restricted by an access device, since the user only has to keep a communication apparatus at hand. The customer can reach this solution without additional hardware and without additional knowledge. During access to the refuse container, an active connection to the central system (for transferring data and authentication) is not necessarily required. Protection against misuse is ensured, since the reproducibility of customary cards (and therefore misuse) is eliminated. Furthermore, access can be both regionally and temporally restricted. The solution can be scaled effectively and easily configured for varying users.

The authentication data preferably give access to a plurality of access devices, in particular refuse containers.

A “predetermined validity range” is preferably understood to mean a validity period. For example, the contract duration between a user and a corresponding waste disposal company is meant.

A “predetermined validity range” can additionally or alternatively also be understood to mean a spatial validity range. Accordingly, a user’s access to a plurality of access devices, preferably refuse containers, within a specific spatial region, for example a household, a community or the like, could be restricted.

A “communication channel” is intended to be understood to mean a transmission path. Such a transmission path connects a transmitter and a receiver. Said transmitter or receiver is advantageously part of a communication interface. The communication apparatus accordingly comprises a first communication interface. The first communication interface is connected to a third communication interface of the data management system via a first communication channel, the “connection” being understood to mean the ability to exchange data. The communication apparatus also comprises a second communication interface, which is connected to the fourth communication interface of the access device by means of the second communication channel, as a result of which at least the authentication data are transferred to the access device by means of wireless technology.

“Access to the access device” can be understood to mean unlocking a refuse lock or unlocking a lock that locks the refuse container, for example.

According to a particularly preferred embodiment, the communication apparatus is a portable data-processing apparatus, for example a mobile phone, a smartphone, a tablet or a laptop. Of course, the present invention is not limited to this list and other similar data-processing apparatus may also be considered for use. Since mobile phones or smartphones are widely used, the vast majority of the members of a corresponding household or community own such a smartphone. The user therefore does not need any other devices for registration or authentication, or must remember corresponding access data.

The communication apparatus preferably comprises a control means, on which software, also referred to as an app, is installed, which app is used to register the user with the data management system and/or by means of which the exchange of data between the communication apparatus and the access device or between the first communication interface of the communication apparatus and the third communication interface of the data

management system via a second communication channel can be controlled. The communication apparatus advantageously comprises a display means

According to another preferred embodiment, the first communication channel is a mobile connection. The mobile connection is preferably a GSM connection or a UMTS connection or a GPRS connection or an LTE connection. Of course, other connections such as radio links, for example in the ISM band or WLAN, are also considered.

According to a particularly preferred embodiment, the wireless connection of the second communication channel, or the wireless technology, is an NFC (near-field communication) connection/technology or an RFID (radio-frequency identification) connection/technology. However, it would also be conceivable to use other wireless technologies, such as Bluetooth or wireless LAN. The second communication interface of the communication apparatus and the fourth communication interface of the data management system are thus provided with the corresponding wireless technology.

The NFC technology and the RFID technology use high-frequency alternating magnetic fields for transferring data. The RFID technology is generally “wireless” transfer. In this case, a passive transponder is used, which is supplied with energy by the alternating field of a reader. Furthermore, the NFC technology also provides “connection-affected” transfer. For connection-affected transfer or Peer-to-Peer transfer, data are transferred between two equivalent transmitters.

Meanwhile, a plurality of commercially available smartphones is equipped with an NFC apparatus. Only two participants can participate in the transfer of data – a so-called initiator, which acts as a transmitter of information, and a receiver, which receives this information.

The NFC technology also provides “wireless” transfer that is analogous to the RFID technology. Such a transfer is often also referred to as passive transfer. In this case, only the initiator generates the high-frequency magnetic field. The receiver can transfer data by means of load modulation. In this case, energy is consumed from the magnetic field by means of a specially adapted resonant circuit of the receiver, upon which the initiator reacts.

In the case of “connection-affected” or active transfer, both the initiator and the receiver generate a high-frequency magnetic field. Firstly, a “handshake” is carried out, in which authentication takes place and in which different settings, such as the optimum transfer speed, for example, are selected. The data are then exchanged. As a result of the

authentication, this active transfer is considered to be substantially more secure than passive transfer.

According to a preferred embodiment, the access device is activated before the data exchange is initiated. This can be done using a button or a similar element, for example. Alternatively, activation can take place by “Low Power Card Detection” (LPCD), by means of which the presence of an NFC-enabled communication apparatus in the direct vicinity is automatically detected.

According to another preferred embodiment, the second communication interface of the communication apparatus has to be activated, i.e. the NFC function is activated.

The software/app preferably remains active in the background so that the NFC function remains activated. The user can therefore gain access to the access device by means of the communication apparatus at any time after successful registration.

According to a preferred embodiment, the access device comprises a second control means, which accordingly triggers an unlocking apparatus if the user has authorisation. In the preferred embodiment as a refuse container, a refuse lock is therefore unlocked. The user can therefore dispose of his waste in the container. When data are exchanged via the second communication channel, the communication apparatus does not need to be connected to the data management system by means of a first communication channel in order to unlock the access device.

According to another preferred embodiment, in step a), user identification data, device identification data relating to the communication apparatus and a registration code, which is provided by an operator, are transmitted to the data management system by means of the communication apparatus.

The authentication data preferably comprise key data, validity information and a region code. The control means of the access device can use these data to check whether access can be granted. If the current time is shown on the control means of the access device, these data can also be used to check the validity period independently of the control means of the communication apparatus.

In this case, the operator is a waste disposal company, a community or the like. The data management system firstly imports the user data from the operator. This user data includes

the name and address of the user, user identification data, such as the contract number, a region code and two registration codes. The registration codes are transmitted to the user by means of a letter, email or the like, for example.

The region code is preferably used to set the spatial validity range.

A predetermined amount of authentication data can preferably be provided to the user. The user can accordingly provide a plurality of communication apparatuses with corresponding authentication data in order to obtain access to the access device by means of a plurality of communication apparatuses.

According to a preferred embodiment, the user identification data and the registration code can be read in by means of a QR scanner of the communication apparatus. This therefore allows for especially quick registration.

When the communication apparatus (5) is used on the access device, the communication apparatus is preferably not connected to the data management system via the first communication channel. This therefore also ensures that the lock is opened in the event of poor or no network coverage at the access device. A regular connection to the data management system is preferably required to regularly extend authentication of the communication apparatus, for which there is a time limit.

According to a preferred embodiment, the communication apparatus comprises a control means, which controls the transmission of the authentication data on the basis of the validity data. Therefore, should the user be in a non-permissible validity range, authentication data are not sent to an access device.

According to a preferred embodiment, the communication apparatus automatically queries the authorisation of the user from the data management system within a predetermined period. The communication apparatus preferably communicates with the data management system via a first communication channel. For safety reasons, it is expedient for the communication apparatus to make contact with the data management system at intervals in order to update the authorisation of the user. If the user does not have authorisation, the authentication data are preferably deleted by a control means of the communication apparatus or the software. The authentication data are accordingly no longer transferred to the access device. The user preferably receives a notification that access is no longer authorised.

The predetermined period can be the predetermined validity period (contract duration) or a shorter period. This period can be predetermined globally or set for specific groups of authentication data, for example for specific regions.

After approximately 50 % of the predetermined period or the validity period, an attempt is preferably made to query the user's authorisation. If a connection to the data management system cannot be established, additional attempts are made.

Shortly before the remaining time, the user is presented with a corresponding notification that a connection to the data management system is required.

Even after the period or the validity period has elapsed, an attempt is preferably still made to periodically make contact with the data management system and to update the authentication data. In addition, a corresponding notification is presented to the user.

According to a preferred embodiment, the user can deregister himself by means of the communication apparatus. In this case, the control unit of the communication apparatus preferably deletes the authentication data on the communication apparatus. The data management system preferably continues to assign the deregistered authentication data to the user, and therefore a history of the user still remains visible.

According to a preferred embodiment, the user can block the authentication data that are assigned to a communication apparatus. When the communication apparatus is used for the first time after the authentication data have been blocked, the access device preferably sends commands by means of the second communication channel to overwrite the authentication data on the communication apparatus. This function is required if the communication apparatus is no longer authorised to gain access to the access device. This can be the case if the communication apparatus is lost or sold or if the owner moves to a different area, for example. The communication apparatus can be identified as a result of the device identification data. The associated authentication data are therefore set to "lost" in the data management system.

If the communication apparatus makes contact with the data management system, the validity period is preferably no longer extended and the user is given corresponding feedback indicating that said communication apparatus may no longer be used.

According to a preferred embodiment, the communication via the second communication channel is an HCE (Host based Card Emulation) communication. The HCE communication has been offered by Android since version 4.4. The HCE communication is based on ISO 14443-A and ISO 7816, i.e. the NFC hardware of the access device always sends a so-called command, to which the communication apparatus responds with a "response". Contact is preferably made between the access device and the communication apparatus as a result of an ISO 7816 Select AID command. Any data can subsequently be exchanged within the command/response pairs.

According to the Select AID command, the communication apparatus answers with the (newest) version of the HCE protocol that is supported on the communication apparatus and the (virtual) UID of the communication apparatus. The Select AID command is processed by the Android system and the app that has been registered for the given aid in the system is started. Should a plurality of apps be registered for the same aid, the user is asked which app is intended to be addressed.

By means of a command, the access device preferably actively asks the communication apparatus whether a "response" is given on the communication apparatus. For HCE communication, the communication apparatus therefore cannot initiate the transfer of data. The communication apparatus preferably responds directly.

The exchange of data between the communication apparatus and the access device preferably consists of transmitting application commands, which consist of a command and data to be transmitted.

According to another preferred embodiment, in order to transmit application commands, a transport protocol is used, by means of which the application commands are broken down into one or more segments depending on the data size of the application command, and transmitted.

According to another aspect of the invention, the object is addressed by an access system for carrying out a method according to any of the preceding embodiments.

The access system can have one or more of the features that are already mentioned with regard to the method. All the features of the method shall therefore also be regarded as having been disclosed with respect to the access system.

Additional advantages, aims and properties of the present invention will be described by means of the following description of the accompanying figures. Identical components can have the same reference numerals in the different embodiments.

In the figures:

Fig. 1 shows an overview of the access system; and

Fig. 2a to 2i show an example sequence of what is displayed on the smartphone when the app is started for the first time.

Fig. 1 shows an overview of the access system (1). A method for operating an access system (1) that comprises an access device (2), in particular for a refuse container (3), is carried out on the access system, said method comprising the following steps:

- a. registering the user (4) using a communication apparatus (5) of a data management system (6) by means of a first communication channel (7);
- b. sending a data record to the communication apparatus (5) by means of the data management system (6) via the first communication channel (7), the data record comprising authentication data and validation data;
- c. initiating the exchange of data between the communication apparatus (5) and the access device (2) via a second communication channel (8), at least the authentication data being transferred to the access device (2), the second communication channel (8) being a wireless connection; and
- d. checking the authentication data for the authorisation of the user using a control means (9) of the access device (2);

the registration being carried out only once and the authentication data authorising access to the access device (2) in a predetermined validity range.

The communication apparatus (5) comprises a control means (10), which controls the transmission of the authentication data on the basis of the validity data.

In the following, the term “app” can also be understood to mean the control means (10) of the communication apparatus (5), since the app is installed on said control means (10) and the control means carries out the corresponding actions.

The app (10) does not need to be manually started in order to open the lock. The app (10) is intended to open automatically and to disappear again after a set time.

All registered key owners are managed in the data management system or web portal. Their smartphone IDs (also called (virtual) key IDs in the following) correspond to the previously used tag IDs. These can also be deactivated/blocked again in the data management system. This may be necessary if a user changes or loses his smartphone or is no longer authorised to access refuse locks. In this case, the ID of the app (10) is entered into a list of banned IDs (blocklist).

Additional required information that still has to be assigned to the keys are: identification features of the smartphone (5) (unique device ID and name of the smartphone) and functions that have to be implemented on the web portal.

The apps have to be distributed. For this purpose, the app is uploaded to an online shop (15) (for example, Google Play Store).

The (virtual) key IDs for the Smartphone app (10) can be generated by a key generator, for example, which ensures the uniqueness of the key ID generated.

In order to be able to use a smartphone (5) as the access key for the access device (2), a registration and authentication process is required and the user ID (generally the contract number) needs to be assigned. For this purpose, provisions have to be made in the data management system (6) and by the community or the waste disposal company (12) for:

- Importing the user data (13) (name, address, contract number, region code, registration code, registration code 2).
- Providing the information letter (14) comprising the registration code and registration code 2 to the user (4) by the community or waste disposal company (12). The contract number should also be visible in this letter. The contract number and the associated registration code should be contained in the letter also as QR code, in order to simplify log-in using the app (10). In order to log in using the app (10), only the QR code then needs to be scanned. The information letter (14) also contains a description of where the app can be downloaded from (recommendation: including second QR code with link to the app in the online shop (15) and how the registration process is carried out).

The information letter (14) informs the user (4) in which app store (15) the virtual key app for the access device can be acquired from and how the smartphone (5) can be registered.

After the app has been downloaded and installed, the user (4) is requested to enter his contract number together with the registration code he has received. Together with a unique ID for the smartphone and the device name, this information is transferred to the data management system by means of a secure connection (https), where they are checked to ensure that they match. In order to increase security, the following additional arrangements are made:

- The registration process is aborted if the registration code is incorrectly entered multiple times. Reactivation of the registration code must then be requested with the support department.
- The maximum number of keys (5) allowed must be specified for every user ID (contract number). A key (5) is a tag, a card or a smartphone (5) with the app installed and NFC activated. The user (4) hereby authenticates himself. This maximum number of keys (5) allowed only includes the keys (5) that are assigned to the user (4) that have the status "active". A user (4) can therefore be assigned any number of keys (5) having a different status (for example "lost"). In this case, the web portal counts every registered smartphone (5) as a key (5) and therefore no more smartphones (5) can be registered using a registration code if the maximum number of (active) keys (5) has been reached.

Provided that the contract number and the registration code match and the maximum number of active keys has not been reached, access-relevant information is transferred to the app (10), the unique key ID (which is selected by the web portal from the pool of available virtual key IDs and set to "active"), the region code, key type, encryption data and validity data, *inter alia*. Some of this information is transferred to the app (10) within an authentication data record, which is created by the data management system. Only this makes it possible to use the smartphone (5) to open an access device having the same region code.

In order to open a refuse lock (2) using a smartphone (5), only NFC has to be activated. The app runs in the background and therefore does not have to be re-started specifically for a disposal. It is sufficient to switch on the smartphone (5). Depending on the embodiment, the smartphone (5) can immediately (i.e. without additional action on the refuse lock (2) or by pressing a button) be held in the detection range of the antenna. As soon as the smartphone (5) has been detected by the refuse lock (2), a notification appears on the screen of the smartphone. The lock opens, provided that the region code and the key status match.

When a smartphone (5) is used on a lock (2), the smartphone (5) does not necessarily have to have a GSM connection. Therefore, this ensures that the lock is opened, even in the event of poor or no network coverage at the location of the refuse lock (2). However, a regular connection to the data management system (6) is required in order to regularly extend authentication of the app (10), which has a time limit. The required regeneration of the authentication data is automatically carried out in the background by means of the virtual key app (10). As a result, the virtual key apps (10) can be deactivated again via the portal if users (4) change or lose the smartphone (5) or are no longer authorised to have access for other reasons.

A virtual key app (10) can also be deactivated by means of the blocking list function of a refuse lock (2) that is already provided. For this purpose, the status of the key ID of the relevant smartphone (5) must be set to “lost” in the data management system (6). After the blocklist has been transferred to the relevant refuse locks (2), the opening function of the app (10) is deactivated if a lost key is detected.

For safety reasons, it is expedient for the app (10) to make contact with the portal at intervals (validity period) and to re-obtain authorisation to open locks (2).

If the key ID of a smartphone (5) is no longer marked as “active” in the web portal (6), the smartphone (5) is no longer given this authorisation – therefore, it is no longer possible to open the lock (2) using this smartphone (5) having this unique identification number. The app (10) deletes the authentication data when authorisation to open the lock is revoked, so that these data are no longer transferred/transferable to a refuse lock (2). The user (4) receives a notification that authorisation to open refuse locks (2) has been revoked.

An example sequence of what is displayed on the smartphone when the app (10) is started for the first time is shown in the following on the basis of Fig. 2a to 2i. If the app is not yet (or no longer) registered, the user is asked to register it:

Fig. 2a: if the device has not been registered yet. The screen for activating the device thus appears. The contract number and the registration code are entered. The data management system (6) checks whether the data are valid. In order for the user not to have to enter the information required by hand, a QR code scanner is provided (Fig. 2b). Every time the app is started, a check is made to see whether NFC is active. The user is made aware if NFC is not active and is given the opportunity to change to the settings (Fig. 2c). If the app has already been registered (and NFC is active), the screen according to Fig. 2d is shown: if the validity

period of the authentication data has expired, a corresponding notification is displayed. If the authentication data have been deleted, the user is made aware of this and then asked to re-register. After successful registration of the app, a help wizard according to Fig. 2e to 2g is displayed, which briefly shows how to use the app.

During the opening process, depending on the status, a success message according to Fig. 2h or a screen having an error message according to Fig. 2i is displayed.

All of the features disclosed in the application documents are claimed as being essential to the invention, provided that they are novel over the prior art, either on their own or in combination.

List of reference numerals

- | | |
|----|--|
| 1 | access system |
| 2 | access device |
| 3 | refuse container |
| 4 | user |
| 5 | communication apparatus |
| 6 | data management system |
| 7 | first communication channel |
| 8 | second communication channel |
| 9 | control means of the access device |
| 10 | control means of the communication apparatus |

Claims

1. Method for operating an access system (1) that comprises an access device (2), in particular for a refuse container (3), said method comprising the following steps:

- a. registering the user (4) using a communication apparatus (5) of a data management system (6) by means of a first communication channel (7);
- b. sending a data record to the communication apparatus (5) by means of the data management system (6) via the first communication channel (7), wherein the data record comprises authentication data and validation data;
- c. initiating the exchange of data between the communication apparatus (5) and the access device (2) via a second communication channel (8), wherein at least the authentication data are transferred to the access device (2), wherein the second communication channel (8) is a wireless connection;
- d. checking the authentication data for the authorisation of the user using a control means (9) of the access device (2);

wherein the registration is carried out only once and the authentication data authorise access to the access device (2) in a predetermined validity range, wherein, when data are exchanged via the second communication channel (8), the communication apparatus (5) does not have to be connected to the data management system (6) by means of a first communication channel (7) and wherein the communication apparatus (5) automatically queries the authorisation of the user from the data management system (6) within a predetermined period, the authentication data on the communication apparatus (5) being deleted and no longer transferred to the access device (2) if the user does not have authorisation.

2. Method for operating an access system (1) according to claim 1, characterised in that

the communication apparatus (5) is a portable data-processing apparatus, which is a mobile phone, a smartphone, a tablet or a laptop, the communication apparatus (5) comprising a control means (10) on which software is installed, which makes it possible to register the user with the data management system and/or by means of which the exchange of data between the communication apparatus (5) and the access device (2) via a second communication channel (8) can be controlled.

3. Method for operating an access system (1) according to either claim 1 or claim 2, characterised in that
the first communication channel (7) is a mobile connection and the wireless connection of the second communication channel is an NFC connection or an RFID connection, the mobile connection being a GSM connection or a UMTS connection or a GPRS connection or an LTE connection.
4. Method for operating an access system (1) according to any of the preceding claims, characterised in that,
in step a), user identification data, device identification data relating to the communication apparatus and a registration code, which is provided by an operator, are transmitted to the data management system (6) by means of the communication apparatus (5), the user identification data and the registration code being read in by means of a QR scanner of the communication apparatus (5).
5. Method for operating an access system (1) according to any of the preceding claims, characterised in that,
when the communication apparatus (5) is used on the access device (2), the communication apparatus (5) is not connected to the data management system (6) via the first communication channel (7).
6. Method for operating an access system (1) according to any of the preceding claims, characterised in that
the communication apparatus (5) comprises a control means (10), which controls the transmission of the authentication data on the basis of the validity data.
7. Method for operating an access system (1) according to any of the preceding claims, characterised in that
the user (4) can deregister himself by means of the communication apparatus (5), the control means (10) of the communication apparatus (5) deleting the authentication data on the communication apparatus (5), the data management system (6) continuing to assign the deregistered authentication data to the user (6).
8. Method for operating an access system (1) according to any of the preceding claims,

characterised in that

the user (4) can block the authentication data assigned to a communication apparatus (5), the access device (2) sending commands to overwrite the authentication data on the communication apparatus (5) by means of the second communication channel (8) when the communication apparatus (5) is used for the first time since the authentication data were blocked.

9. Method for operating an access system (1) according to any of the preceding claims, characterised in that

the communication via the second communication channel (8) is an HCE (Host based Card Emulation) communication, the contact between the access device (2) and the communication apparatus (5) being made by means of an ISO 7816 Select AID command.

10. Method for operating an access system (1) according to claim 9, characterised in that,

by means of a command, the access device (2) actively asks the communication apparatus (5) whether a response on the communication apparatus (5) is given, the communication apparatus (5) responding directly.

11. Method for operating an access system (1) according to either preceding claim 9 or preceding claim 10,

characterised in that,

the exchange of data between the communication apparatus (5) and the access device (2) consists of transmitting application commands, which consist of both a command and data to be transmitted.

12. Method for operating an access system (1) according to any of preceding claims 9 to 11,

characterised in that,

in order to transmit application commands, a transport protocol is used, by means of which the application commands are broken down into one or more segments, depending on the data size of the application command, and transmitted.

13. Access system (1) for carrying out a method according to any of the preceding claims.