Description

Method and device for access control

Technical field

The invention relates to a method and to a device for access control.

Prior Art

From document WO 2006/000618 A2, a method for the wireless input of a destination call for an elevator is known. In this context, a wireless connection is set up between the mobile telephone of the person who has requested an elevator cage with the mobile telephone and the elevator controller in a first step. In a second step, the person and the floor on which the person is located are identified by the elevator controller and the user profile belonging to this person is selected. Subsequently, the elevator controller determines the destination floor by means of the user profile and ensures that an elevator cage is provided for the person on the floor on which he is located, and the destination floor is approached thereafter.

From document JP 2005-280882, an elevator with a safety system is known in which a mobile telephone is used for the identification of a person. So that the person obtains access to the elevator, the identification number indicated on the display panel of the mobile telephone is acquired by means of an optical reader and forwarded to an identification unit. If the identicaton number, and

thus the person, is registered with the identification unit, this person is granted access to the elevator.

Illustration of the invention

It is an object of the invention to specify a method and a device for access control to a building, a building area, a room, an elevator cage or an elevator. This is intended to ensure that only those persons obtain access who are also really authorized for access. Any manipulation for the purpose of misuse is intended to be largely impossible.

The object is achieved by a method for access control having the features as claimed in claim 1.

The method for access control according to the invention comprises the following steps. An identification code is sent to an access node by means of a mobile telephone. If the identification code is recognized as being valid, an access code is sent to the mobile telephone by the access node and presented on the display of the mobile telephone. The access code is detected by means of a camera and if the access code is recognized as being valid, the access is granted.

Advantageous developments of the invention are obtained from the features specified in the dependent claims.

In one embodiment of the method according to the invention, the identification code is the telephone number of the mobile telephone.

In a further embodiment of the method according to the invention, the access code is a two-dimensional optical code.

In a third embodiment of the method according to the invention, the access code is a data matrix code or a QR code.

In addition, it can be provided in the method according to the invention that the identification code is conducted to a control unit by the access node which then checks whether the identification code is contained in a list of permissible identification codes. If this is the case, the access code is conducted to the access node.

In addition, it may be of advantage if in the method for access control, an elevator is released for use when the access has been granted.

In a development of the method according to the invention, the access code is valid for a limited time. This further reduces the risk of misuse.

In another development of the method according to the invention, the access code can be used only once. This further reduces the risk of misuse.

The method according to the invention can be used for the purpose of access control to a building, a building area, an elevator cage or an elevator.

The device according to the invention for performing the method for access control comprises a mobile telephone

and an access node which is constructed and can be operated in such a manner that it can receive the identification code of the mobile telephone and transmit the access code to the mobile telephone. The device also comprises a control unit which is constructed and can be operated in such a manner that it can check the identification code and generate the access code. Furthermore, an optical reader is provided which is connected to the control unit.

In the device according to the invention, the optical reader can be a scanner or a camera.

Finally, a computer program product is proposed which is stored on a medium which can be used by a computer, which contains program code readable by the computer and which ensures that the computer performs the described method for access control. The computer can be a part of the control unit or of the access node.

Brief description of the drawings

In the text which follows, the invention will be explained in greater detail by means of a number of exemplary embodiments, with reference to four figures.

Figure 1 shows a possible embodiment of the device for access control according to the invention in the form of a block diagram.

Figure 2 shows an example of a data matrix code.

Figure 3 shows an example of a QR code.

Figure 4 shows a flowchart for illustrating the method for access control according to the invention.

Figure 5 shows a further example of a method for access control according to the invention.

Approaches for carrying out the invention

In the text which follows, an embodiment of the invention is explained with reference to figures 1 and 4. In figure 1, a possible embodiment of the device for access control according to the invention is shown in the form of a block diagram. Figure 4 shows the flowchart for illustrating an embodiment of the method for access control according to the invention.

For a person to obtain entry or access to a building, a building area such as, for example, a room, or an elevator 9, the person can identify himself at a corresponding access node 2, which will also be called access point AP in the text which follows, by means of their mobile telephone 1. As soon as the person comes within range of the access node 2 with their mobile telephone 1, an identification code ID is sent by the mobile telephone 1 to the access node 2 via a radio link 8 (step S1).

The radio link 8 can be effected, for example, via Bluetooth. Bluetooth is a standard according to IEEE 802.15.1 and is used for the cableless networking of devices over a short distance. In this context, Bluetooth forms the interface via which the mobile telephone 1 and the access node 2 can communicate with one another.

The access node 2 is equipped with a corresponding antenna 2.1 for this purpose. After the access node 2 has received the identification code ID, it forwards it to a control unit 3 (step S2). The control unit 3 can be, for example, a server. The access node 2 and the control unit 3 are arranged spatially separated, as a rule. This is not mandatory. In a building, a number of access nodes 2 can also be located, all of which are then connected to the control unit 3.

The identification code ID is advantageously the telephone number of the mobile telephone 1. However, it can also be provided that the person who uses the mobile telephone 1 must enter a particular code, for example a password, via the keyboard 1.2 of the mobile telephone 1, which is then transmitted to the access node 2 via the radio link 8. In this case, the code entered via the keyboard 1.2 corresponds to the identification code ID.

In a further step S3, the server 3 checks the received identification code ID. If the identification code ID is not considered to be permissible (step S4), the server 3 informs the access node 2 that the person must be denied the access to a particular equipment, such as, for example, an elevator 9 (step S5). If, on the other hand, the identification code ID is considered to be permissible (step S4), the server 3 generates an access code (step S6) and transmits it to the access node 2. The access code will also be called optical code in the text which follows.

The access code can be valid for a limited time. The result is that a person is granted access only for a certain period of time. In addition, it can be provided that the access code is valid only a single time so that, after it has been used once, it can no longer be used a further time. This prevents misuse. Thus, the mobile telephone 1 cannot be used by any other person for obtaining access with the same access code.

Furthermore, the following can be provided. As soon as the person who carries the mobile telephone 1 has been granted access, any further access with the same mobile telephone 1 is blocked for a certain period of time and/or for a certain access node. This prevents that the mobile telephone 1 is handed to another person who then obtains access with this mobile telephone.

As the access code, a data matrix code 6 can be generated, for example, by the server 3. Figure 2 shows an example of such a data matrix code 6. In this context, the term code does not mean the encryption of data in order to keep these secret but the graphical imaging of the data in binary symbols. The data matrix code is a two-dimensional barcode or 2D code which exists in various code schemes, for example "ECC n". ECC stands for error checking and correction algorithm and the following n stands for a value between 0 and 200. The most reliably readable code scheme is the ECC 200 scheme. The size of the square or also rectangular code image is determined from a large selected set, the symbol elements of the code image are square or round. The data matrix code is standardized at the International Standardization Organization (ISO) and described in ISO specifications ISO/IEC

16022:2000 and ISO/IEC 24720:2006 and in other standards for applications such as, for example, in DIN standards and DIN-EN standards. These standards are binding throughout the industry. Using a standardized code ensures that the code can be read independently of the manufacturer of the coder or of the reader.

In the data matrix code 6, the information is coded in a square or rectangular area as patterns of equally large dots. The dots are small black or white boxes which adjoin one another, or round dots with gaps inbetween. Due to the uniform symbol size and the fixed symbol spacing, reading of the image and decoding the information is reliable and the data matrix code is compact in its two-dimensional extent. During the reading of the data matrix code, the arrangement of dots within the border and in the raster of the matrix is detected.

The data matrix code 6 contains redundant data so that, for example, up to 25% errors in the code image can be corrected with a Reed-Solomon error correction in ECC 200. This is of advantage especially when parts of the code image are covered or unreadable.

As an alternative to this, a QR code 7 can also be generated, for example, as access code by the server 3. Figure 3 shows an example of such a QR code 7. The QR code 7 is also a two-dimensional barcode or 2D code, QR standing for Quick Response, that is to say for a fast answer.

In the QR code 7, too, the term code does not mean the secret encryption of data but the imaging of the data in binary symbols. The QR code 7 consists of a square matrix

of black and white dots which represent the coded data in the binary system. A special marking in three of the four corners of the square specifies the orientation. In the QR code, the data are present redundantly so that, even if up to 30% of the QR code are destroyed, it can still be read correctly. Up to 7,089 numeric characters, 4,296 alphanumeric characters or 2,953 bytes can be stored with the QR code 7. The standard for the QR code is found in ISO standard ISO/IEC18004.

Both the data matrix code 6 and the QR code 7 are machine-read by means of an optical reader 5 such as, for example, a scanner or a camera. The data contained in codes 6 and 7 can then be processed further electronically.

After the server 3 has generated the access code 6 or 7, respectively, and transmitted it to the access node 2, the access code 6 or 7, respectively, is sent to the mobile telephone 1 by the access node 2 via the radio link 8 in a step S7.

Following this, the access code 6 or 7, respectively, is presented on the display 1.1 of the mobile telephone 1 in step S8. The user of the mobile telephone 1 can now show this access code to a camera 5 which sends the recorded image with the access code to the server 3 (step S10). The server 3 thereupon checks whether the access code is permissible (step S11). This can be effected, for example, in that the server 3 compares the access code recorded by the camera 5 with the access code sent by the server to the mobile telephone 1. If the access code is considered to be permissible (step S11), the server 3 in-

forms the access node 2 that access is granted to the person (step S12). If, in contrast, the access code is not considered to be permissible (step S11), the access node 2 is informed by the server 3 that the access or the use of a particular item of equipment such as, for example, an elevator 9, must be denied to the person (step S13). If the access to the elevator 9 is denied, the elevator controller 4 which is used for controlling the elevator 9 is informed of this by the control unit 3. The elevator controller 4 thereupon initiates the corresponding measures.

In the present context, the term access is understood to be a generic term which comprises both the entry or access to a building, a room or an elevator cage and the use of a device or equipment such as, for example, an elevator.

Figure 5 shows a sequence scheme of a further example of the method according to the invention according to figures 1 to 4 for access control.

Buildings are secured more and more by electronic access controls. Occupants of the building or assistants who are active in this building are then also visited by persons who do not have access authorization for the building. So that access can be granted to these persons in a simple and efficient manner, the method according to the invention for access control according to figures 1 to 4 can be applied.

In a step 1, an occupant of the building or an assistant who is active in this building places an enquiry to a

control unit 3 for a visitor without access authorization to the building, for setting up or generating a user profile for the visitor by means of a communication unit 10, for example a computer, a PDA, a mobile telephone etc.

The enquiry can contain at least one rule, for example generated by means of a web application, a suitable computer program, a functionality of a date agreement or administration application etc., and sent to the control unit 3. A date agreement or administration application represents, for example, Lotus Notes, Microsoft Outlook etc.

The control unit 3 generates in a second step the user profile in dependence on at least one rule and sends an identification code for the user profile to a mobile telephone 1 of the visitor.

The at least one rule can be of any type. It is specified by the communication unit 10 and/or by the control unit 3. It is conceivable that the at least one rule consists in that no rule is used. It can also depend on safety requirements, needs of the visitor, for example access suitable for handicapped persons, etc., needs of the person visited etc. For example, a time window in which the access is granted so that the access is only temporarily valid can be defined as at least one rule. As well, at least one rule could be that, before an access release is granted, it is checked whether the visitor is located in front of the building. A further rule could be that the visitor, when entering the building, is monitored or tracked by means of suitable monitoring systems along the way to the location of the visited person. If the visitor

is enabled to have access to the building more than once, the access times can be determined by means of the at least one rule. For example, it could be regulated that the visitor should only have access on Friday from 14.00 - 17.00 in each case.

As has already been described in figures 1 to 4, the identification code can be sent to the mobile telephone 1 from the control unit 3 in different manners. For example, it can be contained in a short message, an email, an audio or voice message etc. and consist, for example, of a password, tones, tone sequences, voice, a sequence of letters, a link etc.

The user profile can contain at least one indication which allows the visitor to be authenticated. However, it is also conceivable that the user profile only contains the at least one rule and an option for verifying the identification code.

In a third step, the mobile telephone 1 sends the identification code for requesting an access code to the control unit 3. Optionally, the identification code can be sent by the mobile telephone 1 to the control unit 3 via an access node 2, according to step 3'. This alternative is already described in figures 1 to 4. It is advantageous in this case that it can be determined at the same time whether the visitor is located in the access area of the building.

According to step 4, the control unit 3 checks the identification code obtained from the mobile telephone 1 and compares this code with the user profile and the verifi-

cation options contained therein and/or authentication data of the visitor. For example, the identification code originally sent to the mobile telephone 1, the telephone number, the name, a random value etc. can be used as verification options or authentication data, respectively. For example, hash values could be calculated by means of a suitable algorithm from the original identification code and that sent last, and compared by the control unit 3. If the comparison of the identification code sent last with the user profile or with data deposited or stored in the user profile results in a valid value, the control unit 3 generates and sends to the mobile telephone 1 an access code, for example a sequence of numbers, a two-dimensional code, a QR code, a data matrix code, a bar-code, an image etc.

As an alternative, in accordance with step 4', the access code can also be transmitted by the control unit 3 to the mobile telephone 1 via the access node 2.

The access code, which can be presented on an output device, for example a display, of the mobile telephone is detected by an optical reader 5, according to a fifth step, and sent to the control unit 3 either via the access node 2 according to step 6' or directly according to step 6.

The control unit 3 checks in dependence on the at least one rule in the user profile and/or the user profile, according to step 7, whether the access code is valid or permissible. If the access code is valid, a release of the access is sent to the access node 2 by the control

unit 3 and the access to the building is thus granted to the visitor.

If the user profile contains the at least one rule, that the visited person is to be notified, the control unit 3 sends to the communication unit 10 a notification, for example a short message, an email, a voice message etc., according to step 8, so that the visited person is informed about the arrival of the visitor.

The preceding description of the exemplary embodiments according to the present invention only serves illustrative purposes and not the purpose of restricting the invention. Within the scope of the invention, various changes and modifications are possible without violating the range of the invention and its equivalents. Thus, for example, a scanner can also be used instead of a camera in order to detect the access code 6 or 7, respectively, on the display 1.1 of the mobile telephone 1.

Patent claims

1. A method for access control
which comprises the following steps:
- an identification code (ID) is sent to an access node (2) by means of a mobile telephone (1),
- if the identification code (ID) is recognized as being valid, an access code (6; 7) is sent to the mobile telephone (1) by the access node (2) and presented on the display (1.1) of the mobile telephone (1),
- the access code (6; 7) is detected by means of an optical reader (5), and
- if the access code (6; 7) is recognized as being valid, the access is granted.

2. The method as claimed in claim 1,
in which the identification code (ID) is the telephone number of the mobile telephone (1).

3. The method as claimed in claim 1 or 2,
in which the access code (6; 7) is a two-dimensional optical code.

4. The method as claimed in claim 1, 2 or 3,
in which the access code (6; 7) is a data matrix code (6) or a QR code (7).

5. The method as claimed in one of claims 1 to 4,
- in which the identification code (ID) is conducted to a control unit (3) by the access node (2),
- in which the control unit (3) checks whether the identification code (ID) is contained in a list of permissible identification codes and if this is the case, conducts the access code (6; 7) to the access node (2).

6. The method as claimed in one of claims 1 to 5, in which an elevator (9) is released for use when the access has been granted.

7. The method as claimed in one of claims 1 to 6, in which the access code (6; 7) is valid for a limited time.

8. The method as claimed in one of claims 1 to 7, in which the access code (6; 7) can be used only once.

9. The use of the method as claimed in one of claims 1 to 8, for the purpose of access control to a building, a building area or an elevator (9).

10. A device for performing the method for access control as claimed in one of claims 1 to 9,
- comprising a mobile telephone (1),
- comprising an access node (2) which is constructed and can be operated in such a manner that it can receive the identification code (ID) of the mobile telephone (1) and transmit the access code (6; 7) to the mobile telephone (1),
- comprising a control unit (3) which is constructed and can be operated in such a manner that it can check the identification code (ID) and generate the access code (6; 7), and
- comprising an optical reader (5) which is connected to the control unit (3).

11. The device as claimed in claim 10, in which the optical reader (5) is a scanner or a camera.

12. A computer program product,
- which is stored on a medium which can be used by a

computer,

- which contains program code readable by the computer, and

- which ensures that the computer performs the method as claimed in one of claims 1 to 8.