

**System for security checking or transport of persons by a lift installation and a method for operating this system**

5 The invention relates to a system for safety checking or transport of persons by a lift installation and to a method for operating this system, according to the independent patent claims.

10 Systems for security checking of persons are known. For example, such systems control the entrance/exit of persons to/from buildings, storeys, rooms, etc.

Intelligent systems for transporting persons enable transport, which is controlled by identification, of persons in transport means. The specification EP-0 699 617 discloses a device for controlling a lift installation in which the lift installation is controlled by a person through an identification code. In that case, a recognition device recognises the  
15 identification code and passes it on as a control signal to a processing unit. This reads the control signal and allocates thereto a predefined, desired travel destination. The bearer of the identification code is thus identified and a travel destination is assigned to him or her. The processing unit transmits a corresponding control signal to the lift installation, which then automatically conveys the person to the travel destination.

20 It has now proved to be a disadvantage that unauthorised persons can use the identification code in order to gain access to buildings, storeys, rooms, etc., and in order to be able to be transported by the lift installation.

25 According to the specification WO-01/25128 a person carries a mobile input device which undertakes authentication by speech recognition and checks whether the person is who he or she purports to be. The person also inputs his or her travel destination by way of the mobile input device, which passes on the travel destination as a control signal to a processing unit, which then communicates a corresponding control signal to the lift  
30 installation which automatically transports the person to the travel destination. The relative awkwardness of this input device, which also necessitates an own electrical current supply, is disadvantageous.

35 It is the object of the invention to provide a system for security checking or transporting persons by a lift installation and a method of operating this system, wherein the reliability

of the identification is increased in simple mode and manner with, at the same time, a more user-friendly possibility of input of a travel destination.

This object is met by the invention in accordance with the independent patent claims.

5

The invention fulfils the object in that a person, who is to be transported by a lift installation, is authenticated by detection of at least one authentication signal by at least one mobile authentication device. For this purpose an authentication signal is detected from the person and checked with at least one person reference. If the authentication  
10 signal and person reference correspond, at least one identification code is provided. The identification code is detected by a stationary recognition device. A predefined travel destination or a travel destination input at the recognition device by the person is assigned to the identification code.

15 Advantageously, the mobile authentication device is similar in size and weight to a credit card and the person carries it with them and can use it at any time simply and quickly. For example, a person takes an authentication device, which is similar to a card, with a fingerprint sensor near the lift installation in his or her hand and an authentication of the person and a destination call take place already. In addition, the use of this authentication  
20 device by a single person is very hygienic. Advantageously, the mobile authentication device does not require an own energy source, but is supplied with electrical current by at least one external energy source, which makes this authentication device simple to use and maintain and economic to provide.

25 A biometric signal is used as authentication signal. Advantageously, a fingerprint or a hand geometry or a facial profile or an iris pattern or a retinal scan or a thermogram or a smell or a voice or a signature or pressing a button is used as authentication signal.

Advantageously, the stationary recognition device comprises at least one input means for  
30 input of the travel destination, which can be a known and proven control and display panel with buttons or a touch screen. This has the advantage that the mobile authentication device does not have to contain such input means and can be constructed to be correspondingly small and simple.

Advantageously, the identification code is checked with a user reference in order to establish whether the person is also a registered user of the lift installation. In this identification it is checked whether at least one user reference exists for the detected identification code.

5

Advantageously, in the case of successful association of identification code and user reference at least one control signal is transmitted to the lift installation in order to transport the person to the travel destination. In the case of an unsuccessful authentication or in the case of an unsuccessful identification, at least one alarm signal is transmitted in order to  
10 lock the person in the lift cage or to deny the person access to the travel destination.

Advantageously, in addition to authentication and identification there is carried out an access control in which it is established whether the person also has authorised access to the travel destination. Advantageously, an access authorisation to the travel destination is  
15 checked with at least one access authorisation. The travel destination of the person is advantageously compared with a list travel destinations of the access authorisation. In the case of presence of access authorisation to the travel destination, at least one control signal is communicated to the lift installation in order to transport the person to the travel destination. In the case of unsuccessful access check, at least one alarm signal is  
20 communicated in order to lock the person in the lift cage or to deny the person access to the travel destination.

The invention is suitable for exclusive as also for alternative or supplementary identification of persons in lift installations. For example, for this purpose mobile  
25 authentication devices carried by persons are supplemented by further stationary authentication devices near the lift installation. Such a need exists, for example, in zones with high security requirements, such as banks, military zones of protection, etc.

The invention is explained in detail by way of example in the following on the basis of two  
30 forms of embodiment. In that case, Figs. 1 and 2 each show a basic illustration of a system for security checking or transporting of persons.

In these basic illustrations, a person P is transported by a lift installation A. Authenticatable goods can also be transported instead of a person. The lift installation A can be any lift  
35 installation, which is installed inside or outside a building, with lift cage, drive and lift

control AS. A drive with a lift cage fastened to a conveying cable and a counterweight fastened to the conveying cable are schematically illustrated. All known and proven lift installations can be used. For example, hydraulic lift installations or also such in which the drive is fastened directly to the cage, and naturally also escalators, can be used.

5

An authentication device F detects at least one authentication signal P0 of the person P, checks the authentication signal P0 and provides an identification code P2. The following biometric methods of authentications are preferably used:

- 10 Fingerprint: A fingerprint of the person P is detected, for example scanned. Preferably, the person P places a finger on a surface of the authentication device F, where a fingerprint is photographed by a camera as a grey tone image. The grey tones are preferably binarised or the line widths reduced. Details are marked.
- 15 Hand geometry; Dimensions of a hand of the person P are detected. The person P preferably places at least a part of his or her hand on a surface of the authentication device F, where a three-dimensional silhouette of the hand is photographed by a camera. Protrusions preferably assist in positioning the hand.
- 20 Facial profile: A facial profile of the person P can be detected as a three-dimensional model or as a two-dimensional pattern or as an infrared image as well as a combination of these methods. In addition, black-and-white images or colour images can be detected. The detection angle can vary, thus profile images or frontal images or general perspectives can be detected. In terms of time, a static image or an image sequence can  
25 be detected. The authentication device F photographs at least a part of the facial profile of the person P by a camera.

- Iris profile: A texture of the iris of the person P is detected. Preferably, the person P stands at a spacing of a few decimetres distance in front of the authentication device F and looks into a camera, which camera photographs the iris texture. This photograph is  
30 digitalised to form an iris code. The iris is preferably divided into annular regions and characteristic features are marked.

- Retinal scan: A structure of the veins of the retina of the person P is detected, for example  
35 scanned. The person P preferably stands at a few decimetres distance in front of the

authentication device F and looks into a camera, which camera photographs the structure of the veins of the retina. For this purpose the eye is preferably irradiated with infrared light. The photoreceptive structures of the eye reflect the infrared light, which reflection is photographed. This photograph is digitalised to form a retina code and characteristic features are marked.

Thermogram: Thermal radiation of the person P is detected. Preferably, a thermal camera of the authentication device F records a facial or whole body thermogram.

10 Smell: a smell of the person P is detected by a smell sensor of the authentication device F.

Voice: Vocal pitch or voice break or accents or speech impediments of the person P is or is or are detected. For that purpose the person P speaks into a microphone of the authentication device F and one or more phrases are recorded.

15

Signature: A signature of the person P is detected, for example scanned. The person P writes a signature on a surface of the authentication device F, which signature is photographed by a camera. Preferably, strokes or dynamics or sounds of writing of the signature are marked or determined.

20

Pressing a button: The mode and manner how buttons of a keyboard are pressed by the person P are detected. Preferably, the authentication device F ascertains, by sensors, the force or dynamics of the pressing of the button.

25 Advantageously the authentication device F comprises at least one sensor S for detecting the authentication signal P0, at least one data store B1 for filing the person reference P1, at least one data store for storing a recognition software, as well as at least one computer unit for execution of the recognition software. The sensor S is, for example, a camera for detecting a fingerprint or a hand geometry or a facial profile or an iris profile or a retinal scan or a signature. A sensor S, for example, a thermal camera for detecting a thermogram. The sensor S is, for example, a smell sensor for detecting a smell. The sensor S is, for example, a microphone for detecting a voice. The sensor S is, for example, a button for detecting the pressing of the button. At least one authentication signal P0 is advantageously digitalised and filed in at least one preceding method step as  
30 a person reference P1. With the recognition software there takes place an authentication  
35

by comparison of the detected authentication signal P0 with the filed person reference P1. For example, specific characteristic features of authentication signal P0 and person reference P1 are compared with one another. This is carried out by a standard software which are available to an expert in the field of lifts.

5

The authentication signal P0 is assignable more or less uniquely to a person P or the acceptance on the part of the user to be subjected to an authentication is high to a greater or lesser extent. Thus, the iris pattern can be assigned quite uniquely to a person, but acceptance of an iris pattern authentication is low.

10

In a preferred form of embodiment at least two authentication signals P0 are detected from the person P and checked. Especially in high-security systems - thus in security-conscientious buildings such as banks, military facilities, etc. - several authentication signals P0 are detected from the person P and evaluated. For example, a fingerprint and  
15 an iris pattern of the person P are detected. The uniqueness of the authentication is thereby strongly increased.

Advantageously the authentication takes place before entering the lift cage. Advantageously the authentication device F is used in the immediate vicinity of the lift  
20 installation A. Advantageously the authentication device F and a recognition device E of the lift installation A comprise a transmitting and receiving unit. For example, the authentication device F comprises a transponder which transmits or receives codes by radio signals. For this purpose, typical radio frequencies are 900 MHz to 6 GHz. For example, the authentication device automatically receives at least one recognition signal  
25 from the recognition device E as soon as the receiving unit of the authentication device F is disposed at a spacing of a few decimetres from the transmitting unit of the recognition device E. With knowledge of the present invention, the expert can obviously also use other transmitting and receiving units and other radio frequencies.

30 The authentication device F is mobile, i.e. the person P carries it in size and weight similarly to a credit card and can use it at any time simply and quickly. The use of the authentication device F by a single person is very hygienic. In a first advantageous form of embodiment the authentication device F does not need an own energy source, but uses an external energy source for electrical current supply. For example, the authentication  
35 device F is supplied with current by way of an electromagnetic field. This can take place

by radio via the recognition device E as soon as the authentication device F is disposed at a spacing of a few decimetres from a recognition device E. In a further advantageous form of embodiment the authentication device F is autonomous in terms of energy, i.e. it has an own electrical current supply like a battery, an accumulator, a fuel cell, etc.

5

Advantageously, the authentication device F or the recognition device E comprises at least one output means for the output of an acoustic or optical or mechanical demand signal. For example, an acoustic demand signal in the form of a tone sequence is used, for example an optical demand signal in the form of a light is used, or for example a  
10 mechanical demand signal in the form of a vibration is used. Obviously, demand signals can also be combined with one another and varied.

Advantageously the person P has a predetermined time window in order to undertake the authentication as well as the identification. For example, the authentication by the sensor  
15 S and the recognition software of the authentication device F lasts exactly 15 seconds. Through setting a time window of 60 seconds the person P has sufficient time to also actually undertake this authentication, i.e. to bring the authentication device F into position, to detect an authentication signal, to compare the detected authentication signal with the filed person reference P1 and to transmit the result to the recognition device E. Obviously,  
20 the authentication of the person can also be less than 15 seconds depending on the respective sensor which is used, for example less than 5 seconds, for example less than 1 second.

The result of the authentication is either positive or negative. In the case of positive  
25 authentication, i.e. on correspondence of authentication signal P0 and person reference P1, the output software provides at least one positive authentication signal P1+. In the case of negative authentication, i.e. in the case of non-correspondence of authentication signal P0 and person reference P1, the output software provides at least one alarm signal P13. Advantageously, the identification code P2 is set up and filed in at least one  
30 preceding method step. For example, the identification code P2 is a numerical sequence or a numeral and letter sequence.

Basically, an identification code P2 filed in the authentication device F or an alarm signal P13 of the authentication device F or an authentication code P2 known to the person P is  
35 transmitted. For the first case, the authentication device F advantageously comprises at

least one second data store B2 for filing the identification code P2, at least one data store for storing an output software as well as at least one computing unit for executing the output software. The output software checks the presence of a positive authentication signal P1+ and thereupon provides the filed identification code P2.

5

The transmission of the identification code P2 or of the alarm signal P13 to the recognition device E can take place in numerous ways:

- Thus, it is possible that the authentication device F comprises a transmitting and  
10 receiving unit and communicates the identification code P2 filed in the authentication device F or an alarm signal P13 of the authentication device F by radio to the recognition device E.

- For example, it is also possible that the person P is provided acoustically or optically or mechanically with an identification code P2 or an alarm signal P13 from the  
15 authentication device F with an output means and that the person P inputs the identification code P2 at the input means of the recognition device E.

- Alternatively thereto it is possible that the person P receives, from the authentication device F or the recognition device E with an output means, an acoustic or optical demand signal for entry at the recognition device E of the identification code P2  
20 known to the person P.

- It is also possible that the person P receives, from the authentication device F or the recognition device E with an output means, an acoustic or optical demand signal for entry, by way of an input means of the authentication device F, of the identification code P2 known to the person P.

25

The possibilities of transmission can take place within the time window set by the recognition device E. However, it is also possible that the authentication device F transmits to the recognition device E by radio at least one transmission signal in order to inform the recognition device E about the imminent transmission or in order to set the  
30 recognition device E a time window for transmission of the identification code P2. Finally, it is possible that the authentication device F sends to the recognition device E the positive authentication signal P1+ or the alarm signal P13 as transmission signal.

The transmission possibilities can be combined and varied. For example, it is possible  
35 that the person inputs the identification code P2 by way of an input means of the

authentication device F and the authentication device F transmits this identification code P2 by the transmitting and receiving unit via radio to the recognition device E. For example, it is possible to use acoustic and/or optical and/or mechanical input means of the authentication device F or recognition device E. An acoustic input means is, for example,  
 5 a microphone, an optical input means is, for example, a screen (touchscreen) and a mechanical input means is, for example, a keyboard.

With knowledge of the present invention the expert can realise numerous variations of the authentication device F, the recognition device E or the checking device C. For example,  
 10 the authentication device F can be a component of an every-day portable apparatus for the person, such as a mobile telephone, a wristwatch, a portable computer (laptop, handheld, etc.), a camera, a photographic appliance, a portable radio, a music reproducing appliance (MP3 player, CD player, etc.), etc. In addition, the authentication device F can also be a component of several such appliances. Finally, the authentication device F can  
 15 communicate by way of any radio networks with the recognition device E or also directly with the checking device C. The components of the authentication device F, the recognition device E and also the checking device C are commercially available and inexpensive.

20 The recognition device E is advantageously mounted in stationary position at an entrance to the lift installation A. Advantageously, the recognition device E is a component of a control and display panel of the lift installation A. Advantageously, the control and display panel is mounted near a storey door of the lift installation A. In the form of embodiment of the invention according to Fig. 1, a travel destination P3 of the person P is predefined and  
 25 filed in at least one third data store B3 of the checking device C. In the form of embodiment of the invention according to Fig. 2, the person P inputs a travel destination P3 by way of an input means of the recognition device E.

The identification code P2 and/or the travel destination P3 is or are transmitted by the  
 30 recognition device E to the checking device C. Advantageously, the recognition device E and the checking device C communicate with one another by cable or radio. In that case, the recognition device E and the checking device C can form a single system. For example, a building 20 comprises storeys and a lift installation A with three lifts arranged adjacent to one another. At least one recognition device E per storey is placed near the  
 35 entrances to the lifts. For example, each recognition device E is an insert which is

pushable into a housing of a control and display panel. For example, each control and display panel has at least one bus insert. These bus inserts are connected to a bus system, such as an LON bus. The recognition devices E communicate with one another by way of the bus system. For example, the checking device C is also an insert and  
 5 pushed into one of the control and display panels. In addition, the checking device E communicates by way of the bus system with the recognition devices E.

The checking device C checks the association with at least one filed user reference P4 with the identification code P2 of the person P and checks the presence of at least one  
 10 filed access authorisation P5 to the travel destination P3 of the person P. For that purpose it comprises at least one fourth data store B4 for filing at least one user reference P4, at least one fifth data store B5 for filing at least one access authorisation P5, at least one data store for storing a checking software and at least one computer unit for executing the checking software. The checking device C can be a central remote server. The user  
 15 reference P4 or the access authorisation P5 is set up and filed in at least one preceding method step. For example, the user reference P4 is a numerical sequence or a numerical and letter sequence. For example, the access authorisation P5 consists of a list with travel destinations for which the person P is authorised with respect to access.

20 The checking software checks whether a user reference P4 is filed for the detected identification code P2. For example, specific characteristic features of identification code P2 and user reference P4 are associated with one another. This is carried out by standard software which is available to an expert in the field of lifts.

25 The result of the identification is either positive or negative. In the case of positive identification, i.e. in the case of association of identification code P2 and user reference P4, the checking device C provides at least one positive identification signal P4+. In the case of negative identification, i.e. in the case of non-association of identification code P2 and user reference P4, the checking software provides at least one alarm signal P13.

30

The forms of embodiment, by way of example, of the invention according to Figs. 1 and 2 differ from one another insofar as in the form of embodiment of the invention according to Fig. 1 in the case of presence of a positive identification signal P4+ a predefined travel destination P3 is provided in the checking device C, whereas in the form of embodiment  
 35 of the invention according to Fig. 2 a travel destination P3 is provided at the recognition

device E. For example, the monitoring software checks the presence of a positive identification signal P4+ and thereupon provides the filed, predefined travel destination.

- 5 The checking software now checks whether the person P is authorised to be transported to the travel destination P3 or to gain access to the travel destination P3. For example, the checking software carries out a comparison whether the travel destination P3 is listed on the list of travel destinations of the access authorisation P5. This is carried out by a standard software which is available to an expert in the field of lifts.
- 10 In the case of positive checking of the access authorisation B5, the checking device C transmits at least one control signal P6 to the lift control AS of the lift installation A in order to transport the person P to the travel destination P3. In the case of negative checking of the access authorisation, the checking device C transmits at least one alarm signal P13.
- 15 In the case of presence of an alarm signal P13, different procedures can be carried out. For example, none of the storey doors to the lift installation A is opened for the person P. Independently thereof, a security service can be warned. It is also possible to give the person P access to a lift cage and then, for example, to close the lift door and keep it locked until the security service is on site and undertakes a further checking of the access
- 20 authorisation B5 of the person P. For example, the lift cage is temporarily stopped or moved to a secure and discrete storey, for example a basement floor, where the person P is received by the security service. With knowledge of the present invention, the expert has numerous possibilities of variation. For example, the lift control AS in the case of presence of an alarm signal P13 can grant the person P access to a lift cage, close the lift
- 25 door, move the lift cage to a secure, discrete storey and then simulate a lift breakdown so that the person P does not have any suspicion until the security service is on site for further checking of the access authorisation B5 of the person P.

## Patent Claims

1. A method for security checking or transport of persons by an elevator installation comprising the steps of:
  - a) generating at least one authentication signal associated with a person seeking to use the elevator installation;
  - b) detecting the at least one authentication signal with a mobile authentication device;
  - c) checking the at least one authentication signal with at least one person reference;
  - d) in the case of correspondence of the authentication signal and the person reference, providing at least one identification code;
  - e) detecting the at least one identification code with a stationary recognition device of the elevator installation;
  - f) checking whether at least one user reference exists for the detected identification code; and
  - g) assigning to the identification code one of a predefined travel destination and an input travel destination input at the recognition device by the person.
2. Method according to claim 1, characterised in that the mobile authentication device (F) is supplied with electrical current by at least one external energy source.
3. Method according to claim 1 or 2, characterised in that a biometric signal, advantageously a fingerprint or a hand geometry or a facial profile or an iris pattern or a retinal scan or a thermogram or a smell or a voice or a signature or pressing of a button is used as authentication signal (P0).
4. Method according to one of claims 1 to 3, characterised in that it is checked whether at least one user reference (P4) exists for the detected identification code (P2).
5. Method according to one of claims 1 to 4, characterised in that the travel destination (P3) of the person (P) is checked with at least one access authorisation (B5) and/or the travel destination (P3) of the person (P) is compared with a list of travel destinations of the access authorisation (P5).
6. System for security checking or transport of persons by a lift installation (A), with at least one mobile authentication device (F) which is carried by a person (P) and which detects at least one authentication signal (P0) of the person (P) and checks whether the authentication signal (P0) corresponds with at least one person reference (P1), which authentication device (F) provides at least one identification code (P2) when authentication signal (P0) and person reference (P1) correspond, and with a stationary recognition device (E) of the lift installation (A) which detects the identification code (P2) and assigns to the