



(51) International Patent Classification:

B66B 5/00 (2006.01) **B66B 1/34** (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/EP2018/050618

(22) International Filing Date:

11 January 2018 (11.01.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

17152478.8	20 January 2017 (20.01.2017)	EP
------------	------------------------------	----

(71) Applicant: INVENTIO AG [CH/CH]; Seestrasse 55, 6052 Hergiswil (CH).

(72) Inventor: MICHEL, David; Weihermatt 6, 6343 Rotkreuz (CH).

(81) Designated States (*unless otherwise indicated, for every*

kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every*

kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

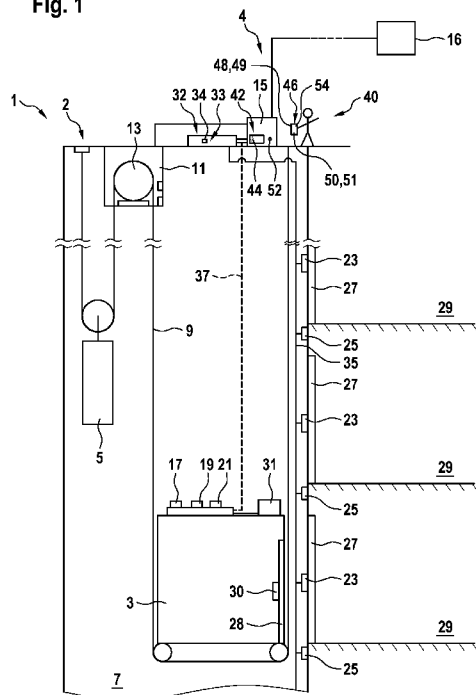
- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND DEVICES FOR AUTHENTICATED CONTROLLING OF SAFETY RELEVANT ACTIONS IN A PASSENGER TRANSPORT SYSTEM

Fig. 1



(57) Abstract: A method for controlling safety-relevant actions, such as resetting an actuated emergency gear (31), in a passenger transport system (PTS) (1) such as an elevator (2) is described. The PTS comprises a safety device (32) for controlling safety-relevant functions and a control device (15) for controlling normal operation functions of the PTS (1). The method comprises: generating an encrypted authentication code (EAC) by the safety device (32); transmitting the EAC to the control device (15); outputting the EAC by the control device (15); optionally: receiving the EAC and decrypting it in a portable decryption device (46) taking into account the time-dependent information for generating the decrypted authentication code and outputting the decrypted authentication code; receiving, by the control device (15), a decrypted authentication code; transmitting the decrypted authentication code to the safety device (32); comparing the decrypted authentication code with the EAC by the safety device (32); controlling the safety relevant actions only if the decrypted authentication code corresponds to the generated EAC. Therein, the EAC comprises time-dependent information which varies over time and which has to be taken into account upon generating the decrypted authentication code. The method allows verifying that a technician (40) is personally on-site at the PTS (1) and is therefore authorized to control safety-relevant actions whereas a technician being off-site e.g. at a remote control centre (16) may not authorize himself as the time-dependent information may not be suitably transmitted to remote locations due to transmission delays, compression losses, etc.

Method and devices for authenticated controlling of safety relevant actions in a passenger transport system

The present invention relates to a method for controlling safety relevant actions, such as resetting a safety device, in a passenger transport system such as an elevator, an escalator or a moving walkway. Furthermore, the invention relates to a passenger transport system configured for authenticated controlling of safety relevant actions and to a passenger transport arrangement comprising such passenger transport system and a portable decryption device.

US 2011/247901 A1 describes an access control method for a passenger transport system.

Passenger transport systems, such as elevators, escalators or moving walkways, serve for transporting passengers within buildings along vertical, inclined or horizontal transport paths, respectively. Therein, severe safety requirements have to be fulfilled in order to guarantee a safety of the passengers.

For example, in a passenger transport system, i.e. in form of an elevator, safe operation conditions are generally continuously monitored by a safety device and in case any unsafe condition is detected, countermeasures are initiated by the safety device. For example, the safety device may comprise or may communicate with numerous monitoring devices such as sensors, detectors, switches, etc. monitoring conditions which are indispensable for a safe operation of the elevator. Such monitoring devices may be for example door switches monitoring an opening/closing state of a door of an elevator car or a door at an elevator floor. Alternatively, monitoring devices may be overspeed sensors sensing an overspeed of the elevator car, path end switches actuated upon the elevator car reaching an end of a transport path in an elevator shaft, etc. Conventionally, all these monitoring devices where included in a series connection of a safety chain such that the safety chain was closed only when all its monitoring devices where in their nominal states. The elevator can only be operated when the safety chain is in a closed state. Alternatively, monitoring devices may communicate with a safety supervision unit (SSU) for example via a safe bus system such as a CAN bus (controller area network). Upon detecting that at least one of the monitoring devices is not in its nominal state, the SSU may assume that the elevator is in an unsafe condition. As a countermeasure, safety relevant actions may be initiated.

For example, the safety device may not only interrupt normal operation of the elevator but may activate for example a safety gear which immediately stops any motion of the elevator car.

5 A safety device having activated the safety gear of an elevator has to be reset to a nominal state before the elevator may resume its normal operation. Upon such reset, e.g. the safety gear is reset and released. However, before such resetting, an actual status and condition of the elevator and its safety gear has to be checked in order to ensure that all elevator components are correctly operating. Regulations may rule that such check has to be
10 performed by a technician being on-site and directly checking the elevator components e.g. by visual inspection of for example the car and/or the safety gear. After having checked a correct status of all relevant elevator components, the technician may reset the safety device. However, in many cases, the safety device itself does not have an own human-machine-interface (HMI). Instead, the safety device may be connected to an
15 elevator control device generally controlling normal operation of the elevator. Such elevator control device typically has an HMI which, on the one hand, enables providing information to a technician and which, on the other hand, enables receiving information from a technician. For example, the HMI may comprise a display for providing information and a keyboard for receiving information.

20 In modern elevators, the elevator control device may be connected to a remote control centre. The control centre may be off-site, i.e. may be distant to the elevator. The elevator control device may then provide all its information is not only to a technician being on-site but may also provide this information for example to technicians being in the off-site control centre. Thereby, remotely controlling the elevator's functions may be enabled
25 such that for example a current status of the elevator may be controlled remotely, i.e. without sending a technician to the elevator for an on-site check. If necessary, control commands may be transmitted from the remote control centre to the elevator control for example for initiating specific actions. Accordingly, status checks may be performed
30 easily and frequently and labour costs may be reduced.

However, while it may be beneficial to monitor at least some of the elevator's functions remotely, not all checks may be performed off-site. As indicated above, at least for some safety critical tasks, a technician may be on-site and check a status of the elevator and its

components personally. Particularly, controlling or initiating safety relevant actions in an elevator may only be allowable after suitable on-site checks. Particularly, resetting a safety device to a normal status after this safety device has initiated safety measures such as actuating the safety gear may only be allowable after a personal check of the elevator system by a technician.

Accordingly, there may be a need for a method for controlling safety relevant actions in a passenger transport system which allows guaranteeing that specific safety relevant actions may only be performed by a person being on-site, i.e. for example a technician being directly at the passenger transport system. Furthermore, there may be a need for a passenger transport system being adapted to perform such method. Additionally, there may be a need for a passenger transport arrangement comprising such passenger transport system and additionally comprising a portable decryption device thereby enabling performing specific embodiments of such method.

Such needs may be met with the subject-matter of the independent claims. Advantageous embodiments are defined in the dependent claims and the following specification.

According to a first aspect of the present invention, a method for controlling safety-relevant actions in a passenger transport system is proposed. The passenger transport system comprises a safety device for controlling safety-relevant functions of the passenger transport system and a control device for controlling normal operation functions of the passenger transport system. The method comprises the following steps, preferably in the indicated order: (a) an encrypted authentication code is generated by the safety device; (b) the encrypted authentication code is transmitted to the control device; (c) the encrypted authentication code is output by the control device; (d) the control device receives a decrypted authentication code decrypted by a portable decryption device; (e) the decrypted authentication code is transmitted to the safety device; (f) the decrypted authentication code is compared with the encrypted authentication code by the safety device; and (g) the safety relevant actions are controlled or executed only if the decrypted authentication code corresponds to the generated encrypted authentication code. Therein, the encrypted authentication code comprises time-dependent information which varies over time and which has to be taken into account upon generating the decrypted authentication code.

According to a specific embodiment of the first aspect of the invention, such method further comprises steps of: (c1) receiving the encrypted authentication code by the portable decryption device; (c2) decrypting the encrypted authentication code in the portable decryption device taking into account the time-dependent information for generating the decrypted authentication code; and (c3) outputting the decrypted authentication code by the portable decryption device. These steps (c1) to (c3) are generally not performed by components of the passenger transport system itself but by the separate portable decryption device and may preferably be inserted between the above mentioned steps (c) and (d).

According to a second aspect of the invention, a passenger transport system comprising a safety device for controlling safety functions of the passenger transport system and a control device for controlling normal operation functions of the passenger transport system is proposed. The passenger transport system is configured for executing a method according to an embodiment of the first aspect of the invention.

According to a third aspect of the invention, a passenger transport arrangement is proposed. Such passenger transport arrangement comprises a passenger transport system according to an embodiment of the second aspect of the invention and a portable decryption device. Therein, the passenger transport arrangement is configured for executing a method according to the above-mentioned specific embodiment of the first aspect of the invention.

Ideas underlying embodiments of the present invention may be interpreted as being based, inter alia, on the following observations and recognitions.

As indicated above, certain safety-relevant actions in a passenger transport system shall only be controllable if it is guaranteed that a technician has previously checked a safe status of components of the passenger transport system. Accordingly, it may be necessary to request an authentication of the technician being on-site. Particularly, it should be avoided that any person, without being on-site but being for example in a distant remote control centre, may control the safety-relevant actions remotely.

Briefly summarised, in order to ensure such on-site authentication, it is suggested that the safety device transmits a specific type of encrypted authentication code to the control device of the passenger transport system which may then output this encrypted authentication code e.g. via its human machine interface. Such encrypted authentication code may then be decrypted by for example a technician being on-site, therefore having access to this HMI. The technician may use a specific portable decryption device for such purpose. The technician may then enter the decrypted authentication code into the control device using e.g. the HMI. The control device may forward the decrypted authentication code to the safety device where it may be compared to the initially generated encrypted authentication code. Thereby, the technician may authenticate his on-site presence. Only upon such authentication, the safety-relevant actions may be controlled or executed.

However, a control device being connected to a remote control centre for example via a network might also transmit the encrypted authentication code to the remote control centre. In such case, for example a technician being in the remote control centre could receive the encrypted authentication code, decrypt it with his decryption device and then send the decrypted authentication code back to the control device. In such scenario, the technician could enable controlling safety-relevant actions without being personally on-site.

In order to prevent such misuse of the remote controllability of the passenger transport system and to ensure that only a technician being actually on-site may initiate controlling safety-relevant actions, it is proposed that the encrypted authentication code is no timely stationary code but comprises time-dependent information. Such time-dependent information shall be part of the encrypted authentication code and shall vary over time. The manner how the time-dependent information varies over time may be predetermined or may be indicated within the encrypted authentication code. Upon decrypting the encrypted authentication code, the decryption device has to take into account this time-dependent information in order to obtain a correct decrypted authentication code.

Accordingly, a technician may obtain the correct decrypted authentication code only in cases where he has access to the correct encrypted authentication code including its time-dependent information. While it is assumed that such correct encrypted authentication code may be output by the control device using e.g. its human machine interface, it is

assumed that upon transmitting the encrypted authentication code for example via a network towards a remote control centre, the time-dependent information comprised therein will be disturbed. The disturbances may result for example from delays and/or runtime errors occurring during transmittance of the code over long distances and/or through various network nodes. Due to such disturbances, the encrypted authentication code will not reach the remote control centre with its original content but with a modified time-dependent information. However, with such modified time-dependent information, the encrypted authentication code may not be correctly decrypted. Accordingly, a technician being off-site e.g. at the remote control centre may not obtain the correct decrypted authentication code and may therefore not remotely enable controlling the safety-relevant actions at the passenger transport system.

Possible options of embodiments of the invention shall now be described in further detail.

The safety-relevant actions to be controlled by the proposed method may be of various types. As an example, resetting of a safety device with a tripped safety gear will be described later herein. Particularly, the example will be described with respect to an elevator. However, the proposed method may also be applied to other actions having a safety critical relevance in a passenger transport system, particularly also in other passenger transport systems than elevators such as escalators or moving walkways. The term “controlling a safety-relevant action” shall be understood herein in a broad sense including e.g. initiating a safety-relevant action and/or enabling control of such safety-relevant action.

In a passenger transport system, the safety device typically monitors conditions being critical for the system’s safety and, based on monitoring results, controls actions of components being relevant for increasing the elevator system’s safety. Inter-alia, the safety device may control a safety gear enabling instant stopping of any motion of the passenger transport system in cases of unsafe conditions.

For such purpose, the safety device itself does generally have to fulfil high safety requirements. For example, any communication of signals between the safety device and its sensors, detectors, actuators, etc. should be safe in a way such as to conform e.g. with high safety integrity levels (SIL). Such communication may typically be established by

dedicated wirings or by a safe communication schemes transmitted over a communication bus system.

5 A passenger transport system generally further comprises a control device. The control device controls functions of the passenger transport system during normal operation. For example, the control device may control driving a car in an elevator system upon receiving requests from passengers within the car or passengers at floors waiting for the car. Accordingly, the control device is generally connected to a drive engine, to a car operating panel (COP) and to landing operation panels (LOPs) of an elevator system.

10 The safety device is generally adapted for controlling specific safety-relevant actions automatically. For example, during normal operation of an elevator, the safety device shall avoid any motion of the elevator car as long as any car door or floor doors are not fully closed and therefore associated door switches are not in their nominal state.

15 Furthermore, there may be extraordinary situations such as e.g. power losses which disturb normal operation of the passenger transport system and its safety device. It is desirable that the passenger transport system and its safety device may automatically recover after for example such power loss without any interaction with a technician being required or, at least, with only an action of a technician being at a remote control centre being required.

20 However, in the specific extraordinary situations, no such automatic or remotely controlled recovery may be allowed but checking the passenger transport system by a technician being on-site may be compulsory. For example, a safety gear is generally automatically actuated upon detecting any unsafe condition in the passenger transport system. According to regulations, it is not allowed to reset the safety gear after such automatic actuation without any preceding on-site check by a technician. Accordingly, it may be necessary to provide a means with which the technician may indicate that he has checked the passenger transport system. Therein, it should be certified that only a technician being actually on-site may correctly authenticate himself.

Typically, the safety device does not comprise an own human machine interface or any other suitable I/O interface. Accordingly, the technician generally may not authenticate

his presence via such safety device's interface. However, the control device is typically provided with a HMI. The safety device may be connected with the control device for suitable signal or data exchange. Such connection may be provided for example via hardwiring, via a bus system, via wireless means, etc. In cases where any interaction
5 between the safety device and for example a human technician is required, the safety device may therefore transmit data to the control device which may then output these data via its HMI or, vice versa, data input to the HMI of the control device may be forwarded to the safety device.

10 In case any interaction with a technician is required, the safety device may generate an encrypted authentication code and transmit it to the control device for output e.g. by the HMI of the control device. The encrypted authentication code may be continuously generated and transmitted or may be generated only upon for example a request made by the technician, for example via an input entered via the control device's HMI.

15 Accordingly, the output encrypted authentication code may be received by the technician. The technician may have a portable decryption device with which he may receive the encrypted authentication code. Accordingly, the encrypted authentication code should be output by the control device in a machine readable manner. The decryption device may
20 then decrypt the encrypted authentication code. For such purpose, the decryption device may have a processor and may be programmed with suitable algorithms for decrypting the encrypted authentication code. Upon such decryption, also the time-dependent information comprised in the encrypted authentication code is taken into account and influences the decryption result. In other words, the encrypted authentication code is not
25 static or stationary but varies over time and the manner in which it varies is part of the information represented by the code. Accordingly, even only slightly modifying a time-behaviour of the encrypted authentication code would mean changing its content, thereby also significantly changing the decrypted code obtained upon decrypting the modified encrypted authentication code.

30 The decryption device may then output the decrypted authentication code. Such outputting may either be performed in a manner such that for example the technician may obtain the decrypted authentication code for example in a form of a sequence of numbers, characters or similar signs. The technician may then enter the decrypted authentication

code into the control device using the control device's HMI. Alternatively, the decryption device may provide the decrypted authentication code in a machine readable manner and may directly submit it to the control device via a suitable interface.

5 Upon having received the decrypted authentication code, the control device forwards this code to the safety device. The safety device may then compare the decrypted authentication code with the original encrypted authentication code. Only when the decrypted authentication code corresponds to the original encrypted authentication code, any controlling or executing of the safety-relevant actions is enabled. When the decrypted
10 authentication code doesn't correspond to the original encrypted authentication code, any controlling or executing of the safety-relevant actions isn't possible or rather blocked.

Accordingly, in the above indicated example, only if the technician is on-site and correctly decrypts the encrypted authentication code using his decryption device on-site,
15 he may authenticate himself and, after having checked the passenger transport system, for example reset the safety gear, i.e. release the safety gear, for subsequently recovering the passenger transport system to normal operation.

According to an embodiment, the time-dependent information varies over time in time
20 intervals shorter than 10 ms, preferably shorter than 5 ms or even shorter than 2 ms.

In other words, the time-dependent information may be represented by a signal which may vary very quickly. While such quickly varying time-dependent information may be correctly output directly by the control device of the passenger transport system, it is
25 generally not easily possible to transmit a quickly varying signal representing such time-dependent information over a network towards for example a remote control centre.

Accordingly, by including a time-dependent information into the encrypted authentication code and including variations in such time-dependent information in time intervals
30 shorter than for example a typical transmission rate in a signal-transmitting network, it may be certified that only encrypted authentication code directly issued at the control device may be correctly decrypted but any encrypted authentication code transmitted via a network may not be correctly decrypted due to the modifications in its time-dependent information which occurred during signal transmission through the network.

The time intervals may be fix, i.e. the time-dependent information may change for example every 10 ms. Excessive deviations from such fixed time intervals may then be interpreted as modifications of the time-dependent information and may be detected by the decryption device. In other words, the decryption device may correctly decrypt the encrypted authentication code only if it receives this encrypted code with time-dependent modifications changing in a correct time interval.

Alternatively, the time intervals may themselves change over time. Such changes may or may not follow a predetermined pattern or algorithm.

According to an embodiment, the encrypted authentication code comprises timing information indicating how the time-dependent information varies over time.

In other words, changes in the encrypted authentication code may follow a predetermined timing scheme or a random timing scheme. Information about this timing scheme may be included in the timing information. Thus, the timing information informs for example about how the time-dependent information will change in a next time interval or has changed in a preceding time interval. Accordingly, the timing information may be taken into account when interpreting the time-dependent information for decrypting the encrypted authentication code.

For example, the timing information may indicate that the time-dependent information will be modified in a next step after a time interval of a specific length. This specific length may vary from step to step during generating and outputting the encrypted authentication code. Accordingly, only if the timing information is correctly received and interpreted, the time-dependent information may be correctly interpreted and taken into account when decrypting the encrypted authentication code.

According to an embodiment, the encrypted authentication code is output by the control device as a visual signal, an acoustical signal or an electromagnetic signal.

In other words, the encrypted authentication code may be output by the control device in various manners. All these manners are preferably adapted for transmitting signals or information in a machine readable way.

For example, the encrypted authentication code may be issued in a visual manner. As one option, the code may be displayed e.g. on a screen being part of the HMI of the control device. Alternatively, the code or at least a portion representing its time-dependent information may be output via a light source such as an LED. Such visualised authentication code may be received by the decryption device for example using a camera, one or a set of photodiodes, or any other type of visual sensor/detector.

As another example, the encrypted authentication code may be issued in an acoustic manner. As one option, the code may be issued as sound wherein the time-dependent information is included for example by corresponding frequency modulations and/or amplitude modulations.

As yet another example, the encrypted authentication code may be issued in an electromagnetic-signal manner, i.e. with an electromagnetic signal being emitted by the control device and being received by the decryption device. The electromagnetic signal may be modulated in accordance to a suitable signal protocol. For example, the encrypted authentication code may be transmitted between the control device and the decryption device via Bluetooth communication or similar means.

According to an embodiment, the encrypted authentication code is output by the control device as a sequence of images.

In other words, the encrypted authentication code may be formed by various images displayed in a time sequence. The images may be displayed for example on a display, preferably a coloured display, provided at the control device. Such display may be fast enough, i.e. may have a sufficiently high refresh rate, such as to display the sequence of images with intended time intervals of e.g. less than 10 ms between subsequent images. Therein, each image may itself include encrypted information. Further information may be comprised in the specific type of the time sequence in which images are displayed.

The sum of both types of information may form the entire encrypted authentication code such that both, the images as well as time intervals between the images, may have to be acquired and interpreted correctly in order to obtain the decrypted authentication code.

The images may be one of various types applicable for representing encrypted information. In other words, the images may be optical, machine-readable representations of data. For example, the images may represent a bar code, a QR code and/or a photoTAN.

5

Bar codes systematically represent data by varying widths of and/or distances between generally parallel lines. Accordingly, bar codes may be referred to as linear or one-dimensional (1D). In specific implementations, two-dimensional (2D) codes may be used, using rectangles, dots, hexagons and other geometric patterns in two dimensions, usually called bar codes although they do not use bars as such. Bar codes may be scanned for example by special optical scanners. Alternatively, any devices that could acquire and analyse images, such as smartphones with cameras, may be used as bar code scanners.

10

QR codes are a specific type of matrix bar code or two-dimensional bar code typically using four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store or represent information. Generally, a QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera. The required data may then be extracted from patterns that are present in both horizontal and vertical components of the image.

15

20

A photoTAN (Transaction Authentication Number) is a specific type of coloured bar code which is used, inter-alia, in authentication processes for online banking. Therein, dots in a two-dimensional pattern may have various colours thereby providing additional options for information encryption. Typically, a photoTAN encrypts a 4- to 8-digit number. After decryption, such number may be displayed for example on a display of the decryption device and may then be for example input by a technician into the HMI of the control device comprising a keyboard.

25

According to another embodiment, at least the time-dependent information may be output as a sequence of light emissions.

30

In other words, at least the time-dependent information being part of the encrypted authentication code may be output by successive light flashes. Therein, the light flashes may differ in intensity, time length or other optical characteristics such that, by varying

these parameters, time-dependent information may be included in the sequence of light emissions.

For example, the light emissions may be emitted by any type of controllable light source.

5 As a very simple implementation, time-dependent information may be output by switching on and off a light source such as a light emitting diode (LED).

10 In principle, the entire encrypted authentication code may be output using such timely varying light emissions. However, the encrypted authentication code may also be a combination of a static part such as a static image (e.g. a static QR code or photoTAN) e.g. displayed on a screen and a dynamic part such as light emissions of timely varying intensity to be emitted e.g. by a “flickering” LED.

15 The transport system according to the second aspect of the invention may be specifically configured such that it may perform one of the described embodiments of the method for controlling safety-relevant actions.

20 According to an embodiment of the passenger transport system, the safety device comprises a computing unit being configured for generating the encrypted authentication code including the time-dependent information.

25 In other words, the computing unit of the safety device is specifically adapted for generating a specific type of encrypted authentication code which is not stationary but which is dynamic and includes the time-dependent information. Therein, as described above, the time-dependent information may be incorporated into the encrypted authentication code in various manners. For example, the time-dependent information may be included in the time intervals between successive images, each of the images representing themselves encrypted information for example in the form of a QR code or a photoTAN. Alternatively, the time-dependent information may be included into a
30 separate signal being independent of any image-representing signal, such separate signal is for example a time-dependent light emission of an LED.

The computing unit may also be adapted for comparing the originally generated encrypted authentication code with the decrypted authentication code.

According to an embodiment of the passenger transport system, the control device comprises a display being configured for displaying the encrypted authentication code including the time-dependent information.

5 Such display may be configured for example such as to be fast enough, i.e. have a sufficiently high refresh rate, such as to display images representing the encrypted authentication code including the time-dependent information with no excessive time delay. For example, the display may be adapted for representing images with a refresh
10 rate of more than 100 Hz, preferably more than 200 or even more than 500 Hz. The display may comprise a one-dimensional or preferably two-dimensional array of pixels, preferably colour pixels. A number of pixels may be low as no complicated images have to be represented with high resolution. For example, a display with 100 x 100 or less pixels or even only 30 x 30 or less pixels may be sufficient.

15 According to an embodiment, the passenger transport system further comprises a light emitting device being configured for emitting a sequence of light emissions representing the time-dependent information of the encrypted authentication code.

Similarly to the above-mentioned display, such light emitting device should be fast
20 enough such as to emit the sequence of light emissions accurately in time, i.e. without excessive time delays. The light emitting device may be a simple but fast LED. For example, a separate LED may be provided at the control device, for example next to a display of the control device. In some cases, the control device already comprises specific LEDs for other purposes such as for example for indicating bridging of an elevator door.
25 For implementing the method described herein, it may be easiest to use such already existing LEDs for emitting the time-dependent information to be included in the encrypted authentication code.

While the passenger transport system itself may generate the encrypted authentication
30 code and may compare it with a decrypted authentication code, it may generally not decrypt the authentication code itself.

In an embodiment of the passenger transport arrangement described herein, this task is to be done by the portable decryption device. Such portable decryption device shall be

brought with and handled by the technician upon inspecting the passenger transport system in order to, after having approved the system's correct operation, authenticate himself in order to for example reset a previously activated safety gear.

5 Therein, the portable decryption device may comprise a signal reception unit, a computing unit and a signal emission unit. These units may be configured for receiving the encrypted authentication code outputted by the control device, then decrypting the encrypted authentication code in the portable reception device taking into account the time-dependent information comprised in the encrypted authentication code, thereby
10 generating the decrypted authentication code, and finally outputting the decrypted authentication code.

In other words, the portable decryption device may be provided with suitable technical components such as at least one signal reception unit such as a sensor or interface for
15 receiving the encrypted authentication code, at least one computing unit such as a processor for decrypting the encrypted authentication code and at least one signal emission unit such as an actor or interface for outputting the decrypted authentication code.

20 The signal reception unit for receiving the encrypted authentication code may be any sensor which is adapted for receiving a physical signal representing the encrypted authentication code. For example, if the encrypted authentication code is issued via a visual signal, the sensor may be a light-sensitive sensor. Particularly, the sensor may be a camera adapted for acquiring a two-dimensional image of e.g. a photoTAN represented
25 on a display of the control device. Alternatively, the sensor may be a simple light-sensitive diode which may sense a light intensity of e.g. modulated light emissions emitted for example by an LED of the control device. In other examples where the encrypted authentication code is issued as an acoustical signal, the sensor may be a microphone or similar device. In cases where the encrypted authentication code is output
30 as an electromagnetic signal, the sensor may be an antenna or similar device. The sensor should be operable in a fast manner such as to avoid any delays in receiving, transmitting and finally decrypting the encrypted authentication code in the decryption device.

The processing unit may be a specifically dedicated processing unit configured for decrypting the encrypted authentication code. Alternatively, the processor may be a general-purpose processor which may be adapted for decrypting the encrypted authentication code via executing suitable software. Particularly, the processor may be adapted for taking into account the time-dependent information comprised in the encrypted authentication code upon decrypting same. In other words, the processor may not only analyse any static data and/or signals but analyse also a time sequence of such data/signal and/or time intervals between subsequent data/signal.

The signal emission unit may be implemented in various ways. For example, the signal emission unit may be a human machine interface, such as a display, via which the decrypted authentication code may be output in a human-readable manner. The technician may then input the decrypted authentication code into another HMI, such as e.g. a touchscreen, provided at the control device such that the control device may then forward this decrypted authentication code to the safety device. Alternatively, the signal emission unit could be adapted for directly transmitting the decrypted authentication code to the control device using for example an interface such as a wireless data communication.

For example, the portable decryption device may be a dedicated device specifically provided with the mentioned components and configured for executing the process steps of receiving the encrypted authentication code, decrypting it and then outputting it. Alternatively, the portable decryption device may be a general-purpose device such as a smart mobile phone comprising multiple sensors, a processor and then output unit, wherein such general-purpose device may be adapted for executing the mentioned process steps by suitable software, for example by a dedicated app.

Upon having been called for inspecting the passenger transport system in reaction for example to the safety gear having been activated, the technician can then bring with him the portable decryption device. After having inspected the relevant components of the passenger transport system, he may bring this decryption device into suitable interaction with the control device of the passenger transport system, for example by focusing the camera of the decryption device onto the display of the control device. An encrypted authentication code generated in the safety device and visually output by the control device via the display may then be received by the decryption device via its camera and

may be decrypted. The decrypted code may then be input into the control device, for example by the technician entering a string of numbers corresponding to the decrypted authentication code into a keyboard or a touchscreen provided at the control device.

5 It shall be noted that possible features and advantages of embodiments of the invention are described herein partly with respect to a method and partly with respect to a device or arrangement for controlling safety-relevant actions in a passenger transport system. One skilled in the art will recognize that the features may be suitably transferred from one embodiment to another and features may be modified, adapted, combined and/or
10 replaced, etc. in order to come to further embodiments of the invention.

In the following, advantageous embodiments of the invention will be described with reference to the enclosed drawing. However, neither the drawing nor the description shall be interpreted as limiting the invention.

15

Fig. 1 shows an elevator according to an embodiment of the present invention.

The figure is only schematic and not to scale.

20 Fig. 1 shows a passenger transport system 1 implemented as an elevator 2 according to an embodiment of the present invention.

The elevator 2 comprises an elevator car 3 and a counterweight 5 arranged in an elevator shaft 7. The elevator car 3 and the counterweight 5 are suspended by a suspension
25 traction means 9 comprising several ropes or belts. The suspension traction means 9 is driven by a traction sheave 13 of a drive engine 11.

A normal operation of the drive engine 11 is controlled by an elevator control device 15. Accordingly, the control device 15 may control a displacement of the elevator car 3
30 between various floors 29 of a building. The control device 15 may also control opening/closing motions of floor doors 27 and/or of a car door 28.

The control device 15 may be connected to a remote control centre 16 being off-site, i.e. being for example in another building or even another city. Signals may be transmitted

from the control device 15 to the remote control centre 16, for example for informing about a current status of the elevator 2, or, vice versa, from the remote control centre 16 to the control device 15, for example for influencing its control functions.

5 In order to be able to control functions of the elevator 2 and/or to guarantee its safety, the elevator 2 comprises a multiplicity of car sensors 17, 19, 21, 30 and shaft sensors 23, 25. For example, an acceleration sensor 17, a position sensor 19, a car velocity sensor 21 and a car door switch 30 are provided at the car 3 and may provide their sensor signals to shaft-based devices, such as the control device 15 or a safety device 32, for example via a
10 hardwired or wireless data linkage 37. Shaft sensors 23, 25 are positioned stationary within the elevator shaft 7 and may provide signals to the control device 15 for example via a bus system 35. For example shaft door contacts 23 may be provided at each of a multiplicity of shaft doors 27 arranged at each of floors 29 of a building. These shaft door contacts 23 may determine whether or not an associated shaft door 27 is correctly closed.
15 Furthermore, door zone contacts 25 may be provided. These door zone contacts 25 may determine whether or not the elevator car 3 is currently in close neighbourhood to one of the shaft doors 27.

20 Signals of the multiplicity of sensors 17, 19, 21, 23, 25, 30 may be processed within a safety device 32, sometimes also referred to as an elevator safety supervising unit (SSU) 33. The safety device 32 is configured to suitably process these sensor signals and to suitably control elevator safety components such as the safety gear 31. Accordingly, while the control device 15 controls operations of the elevator 2 during normal operation, the safety device 32 controls safety-relevant functions upon detecting sensor signals
25 which indicate a safety critical situation. For example, the safety device 32 may control activation of the safety gear 31 and may for example actuate a safety gear.

Typically, safety-relevant actions may be controlled only by the safety device 32. As releasing a safety gear generally is a safety-relevant action, once activated, it may not be
30 allowed to reset the safety gear 31 with its actuated safety gear without a technician 40 (not represented to scale in the figure) previously having checked the elevator 2 and having determined for example reasons for the activation of the safety gear 31. Particularly, it may be indispensable to assure that the technician 40 may not reset the safety gear 31 from a remote location such as the remote control centre 16 but has to

personally check the status of the elevator 2 on-site. Same may be true for other safety-relevant actions in the elevator 2.

Accordingly, the method as proposed herein for controlling safety-relevant actions may be implemented in the elevator 2 for assuring that a technician 40 is personally present at the elevator 2, i.e. is on-site.

It is planned that a safety gear reset procedure may be performed by the control device 15 in order to make things easier for the technician 40. For example, the technician may choose a menu on the control device 15 to start the safety gear reset procedure.

Thereupon, the control device 15 sends a message to the safety device 32 indicating that someone appears to be on-site and the safety gear reset procedure may be started.

However, because the control device 15 does generally not fulfil high safety requirements, a mechanism is needed to ensure the on-site attendance of the technician 40.

For this purpose, at the beginning of the safety gear reset procedure, the safety device 32 first generates an encrypted authentication code. As the safety device 32 generally has no output unit or human machine interface, this code is then transmitted to the control device 15. The control device 15 may output the encrypted authentication code. For example, the control device 15 may display the encrypted authentication code on its display 42 as a sequence of images 44. Each image may for example represent a photoTAN which represents part of the information included in the encrypted authentication code and is represented by a two-dimensional pattern of coloured dots. The photoTAN may be photographed by a camera 48 serving as a signal reception unit 49 of for example a smart mobile phone serving as a portable decryption device 46. Upon having received the photoTAN, the decryption device 46 may decrypt the photoTAN.

However, as the photoTAN conventionally comprises encrypted information in a static format such that the photoTAN could easily be transmitted for example to the remote control centre 16, it is proposed to include a dynamic component into the encrypted authentication code which may not easily be transmitted for example via a network to the remote control centre 16. Thereby, any decrypting of the encrypted authentication code at a remote location may be prevented, as such dynamic component generally may not be

transmitted via a network without any transmission delays significantly modifying its content. Particularly, upon transmitting and displaying such dynamic component to a remote control centre 16, delays have to be expected which prohibit to start a safety gear reset procedure remotely because no correct decrypted authentication code will be generated due to wrong timing, missing iterations and/or loss of information due to compression.

In other words, in the present example, not only a single image comprising a photoTAN is displayed on the control device's 15 display 42, but a sequence of such images is displayed in short time intervals of for example less than 10 ms. Therein, the multitude of varying images and/or the time intervals between such images may form the dynamic component of the encrypted authentication code, i.e. the time-dependent information comprised in the encrypted authentication code.

In addition or as an alternative, the time-dependent information forming the dynamic portion of the encrypted authentication code may also be output in other ways. For example, a light emitting device 52 such as an LED provided at the control device 15 may be operated such as to emit a sequence of light emissions representing the time-dependent information. In other words, the LED may act as an additional pixel for example in addition to the coloured dots of a photoTAN. The LED may have the states on, off or dimmed. To help the decryption device to find the LED, markings may be provided on the control device 15 or a printed circuit board thereof.

Upon decrypting the encrypted authentication code in the decryption device 46, the time-dependent information has to be taken into account in order to come to the correct decryption result. For this purpose, a computing unit 54 comprised in the decryption device 46 processes the received encrypted authentication code in accordance with a predetermined algorithm.

The decrypted authentication code may then be displayed as a multiple digit number on a display 50 forming a signal emission unit 51 of the decryption device 46. The technician 40 may read such number and input the number into the control device 15 for example via a keyboard or via the display 42 being implemented as a touchscreen.

The decrypted authentication code may then be forwarded to the safety device 32.

Finally, the safety device 32 may compare this decrypted authentication code with the originally generated encrypted authentication code. Only when the decrypted and the encrypted authentication code correspond to each other, the safety device 32

5 acknowledges that the technician 40 is actually on-site and allows controlling the safety-relevant actions, i.e. starts the safety gear reset procedure.

Thus, with the method proposed herein and with a passenger transport system 1 or a passenger transport arrangement 4 additionally including the portable decryption device

10 46, authentication of a technician 40 being on-site may be reliably enabled. The method allows verifying that a technician 40 is personally on-site at the passenger transport system 1 and is therefore authorized to control safety-relevant actions. In contrast hereto, a technician being off-site e.g. at a remote control centre 16 may not authorize himself, as the time-dependent information comprised in the encrypted authentication code may not
15 be suitably transmitted to remote locations due to transmission delays, compression losses, etc.

Finally, it should be noted that the term “comprising” does not exclude other elements or steps and the “a” or “an” does not exclude a plurality. Also elements described in
20 association with different embodiments may be combined. It should also be noted that reference signs in the claims should not be construed as limiting the scope of the claims.

Claims:

1. Method for controlling safety-relevant actions in a passenger transport system (1),
5 the passenger transport system (1) comprising a safety device (32) for controlling safety-relevant functions of the passenger transport system (1) and a control device (15) for controlling normal operation functions of the passenger transport system (1), the method comprising:
generating an encrypted authentication code by the safety device (32);
10 transmitting the encrypted authentication code to the control device (15);
outputting the encrypted authentication code by the control device (15);
receiving, by the control device (15), a decrypted authentication code decrypted by a portable decryption device (46);
transmitting the decrypted authentication code to the safety device (32);
15 comparing the decrypted authentication code with the encrypted authentication code by the safety device (32);
controlling the safety relevant actions only if the decrypted authentication code corresponds to the generated encrypted authentication code;
wherein the encrypted authentication code comprises time-dependent information which
20 varies over time and which has to be taken into account upon generating the decrypted authentication code.
2. Method of claim 1, wherein the time-dependent information varies over time in time intervals shorter than 10ms.
25
3. Method of one of the preceding claims, wherein the encrypted authentication code comprises timing information indicating how the time-dependent information varies over time.
- 30 4. Method of one of the preceding claims, wherein the encrypted authentication code is output by the control device (15) as one of a visual signal, an acoustical signal and an electromagnetic signal.

5. Method of one of the preceding claims, wherein the encrypted authentication code is output by the control device (15) as a sequence of images (44).
6. Method of claim 5, wherein the images represent one of a bar code, a QR code and a photoTAN.
7. Method of one of the preceding claims, wherein the time-dependent information is output as a sequence of light emissions.
8. Method of one of the preceding claims, further comprising:
receiving the encrypted authentication code by a portable decryption device (46);
decrypting the encrypted authentication code in the portable decryption device (46) taking into account the time-dependent information for generating the decrypted authentication code; and
outputting the decrypted authentication code by the portable decryption device (46).
9. Passenger transport system (1) comprising a safety device (32) for controlling safety functions of the passenger transport system (1) and a control device (15) for controlling normal operation functions of the passenger transport system (1), the passenger transport system (1) being configured for executing a method according to one of claims 1 to 8.
10. Passenger transport system of claim 9, wherein the safety device (32) comprises a computing unit being configured for generating the encrypted authentication code including the time-dependent information.
11. Passenger transport system of claim 9 or 10, wherein the control device (15) comprises a display (42) being configured for displaying the encrypted authentication code including the time-dependent information.
12. Passenger transport system of one of claims 9 to 11, further comprising a light emitting device (52) being configured for emitting a sequence of light emissions representing the time-dependent information of the encrypted authentication code.

13. Passenger transport arrangement (4) comprising:
a passenger transport system (1) of one of claims 9 to 12; and
a portable decryption device (46);
the passenger transport arrangement (4) being configured for executing a method
according to claim 8.

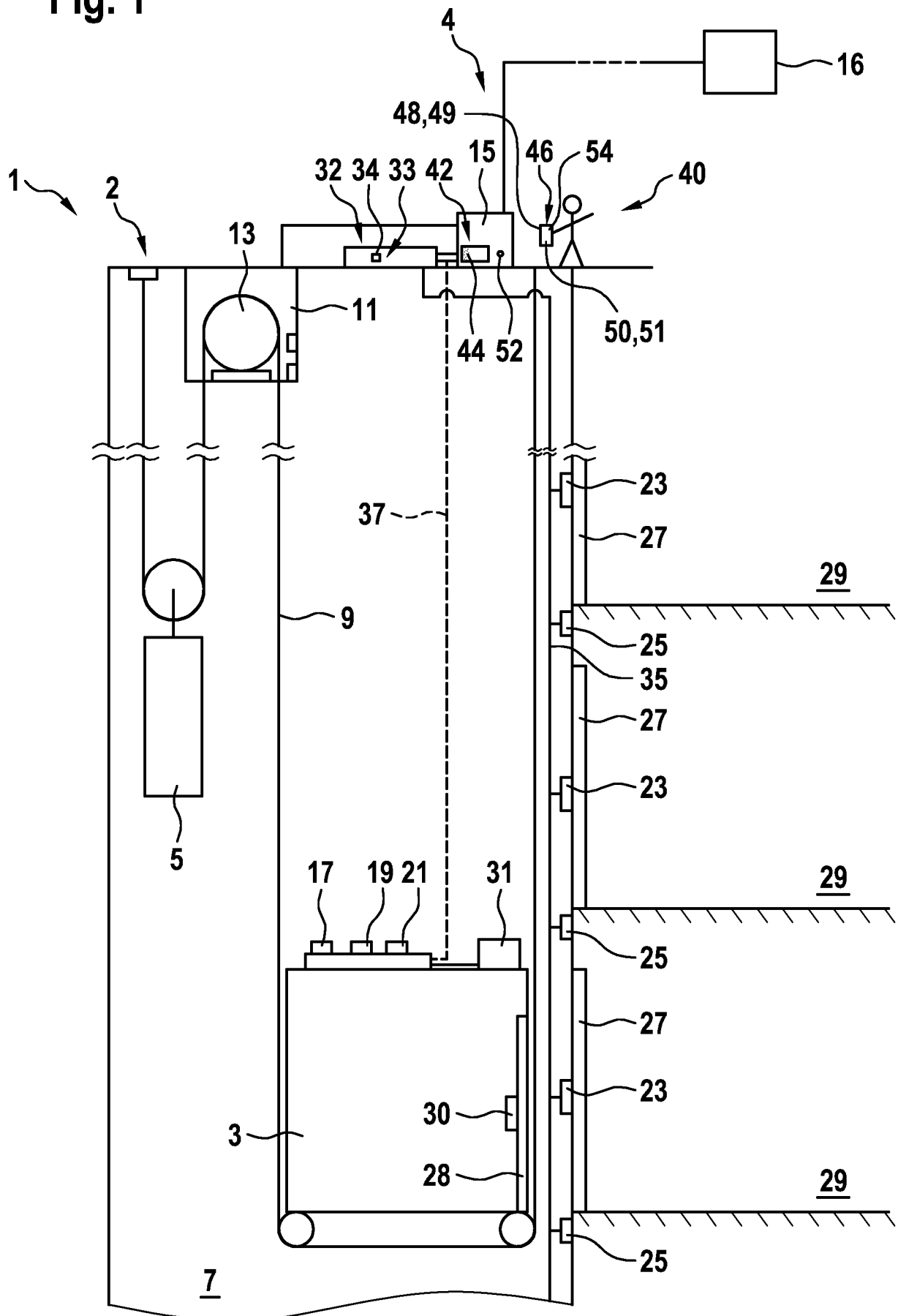
5

14. Passenger transport arrangement of claim 13, wherein the portable decryption
device (46) comprises a signal reception unit (49), a computing unit (54) and a signal
emission unit (51) being configured for
receiving the encrypted authentication code output by the control device (15);
decrypting the encrypted authentication code in the portable reception device (46) taking
into account the time-dependent information comprised in the encrypted authentication
code, thereby generating the decrypted authentication code; and
outputting the decrypted authentication code.

10

15

Fig. 1



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/050618

A. CLASSIFICATION OF SUBJECT MATTER
INV. B66B5/00 H04L9/32 B66B1/34
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B66B H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011/247901 A1 (WILKE MICHAEL [DE] ET AL) 13 October 2011 (2011-10-13) the whole document	1-14
Y	----- Anonymous: "Transaktionsnummer - Wikipedia", 21 December 2016 (2016-12-21), XP055383212, Retrieved from the Internet: URL:https://de.wikipedia.org/w/index.php?title=Transaktionsnummer&oldid=160868121 [retrieved on 2017-06-20] paragraph [01.6] - paragraph [01.7] ----- -/-	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

16 April 2018

Date of mailing of the international search report

07/05/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Fiorani, Giuseppe

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2018/050618

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Anonymous: "Time-based One-time Password Algorithm - Wikipedia, the free encyclopedia", 12 October 2014 (2014-10-12), XP055461415, Retrieved from the Internet: URL:https://web.archive.org/web/20141012132024/http://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm [retrieved on 2018-03-21] -----	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2018/050618

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011247901 A1	13-10-2011	BR PI0823337 A2	23-06-2015
		CN 102257536 A	23-11-2011
		EP 2368229 A1	28-09-2011
		KR 20110084552 A	25-07-2011
		RU 2011124771 A	27-01-2013
		US 2011247901 A1	13-10-2011
		WO 2010069347 A1	24-06-2010
