(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 4 443 401 A1

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
09.10.2024 Bulletin 2024/41

(21) Application number: **23166638.9**

(22) Date of filing: **04.04.2023**

(51) International Patent Classification (IPC):
G07C 9/00 *(2020.01)*

(52) Cooperative Patent Classification (CPC):
G07C 9/00309; G07C 2009/00373;
G07C 2009/0065; G07C 2009/00793

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA
Designated Validation States:
KH MA MD TN

(71) Applicant: **dormakaba Schweiz AG**
8623 Wetzikon (CH)

(72) Inventors:
- **Duetschler, Urs**
  8620 Wetzikon (CH)
- **Studerus, Paul**
  8165 Oberweningen (CH)
- **Mueller, Markus**
  8153 Rümlang (CH)
- **Buholzer, Martin**
  8620 Wetzikon (CH)

(74) Representative: **Balder IP Law, S.L.**
Paseo de la Castellana 93
5a planta
28046 Madrid (ES)

(54) **WAKEUP FOR ACCESS ENFORCEMENT POINT(S)**

(57) According to a first aspect of the present invention, a computer-implemented wakeup method is provided, being performed by an access enforcement point. The access enforcement point may be configured to cause operation, preferably unlocking and/or locking, of an access point. The access enforcement point may comprise energy harvesting means that may include a solar cell and an energy storage. The method may comprise harvesting ambient light and generating, by the solar cell, a solar cell signal. The method may comprise determining that the solar cell signal satisfies a mode switching condition. The method may comprise, in response to determining that the solar cell signal satisfies a mode switching condition, switching the access enforcement point from a sleep mode into an active mode. The mode switching condition may comprises a drop of the solar cell signal that may correspond to a reduction of ambient light incident on the solar cell that may occur upon manually masking the solar cell.

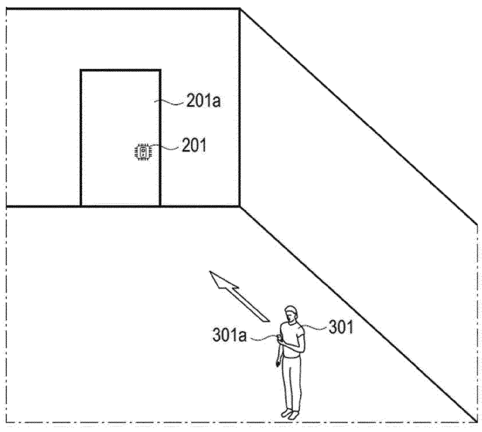


Fig. 1

EP 4 443 401 A1

Description

FIELD OF THE INVENTION

[0001] The present invention relates to a wakeup method for an access enforcement point or a plurality of access enforcement points, in particular to an energy-efficient wakeup method. Further, the present invention relates to using an access enforcement point in a wakeup method. Further, the present invention relates to a corresponding computer program.

BACKGROUND OF THE INVENTION

[0002] Entry systems have become widely used in applications in particular for access control in building facilities. Access control relates to granting, denying or limiting access to particular section(s) of a controlled area, usually by means of some level of access control by use of a barrier, such as a door, turnstile, parking gate, elevator door, or other barrier.

[0003] Various prior art systems are known for access control based on various principles using corresponding technologies. According to a first known approach, referred to as "who you are", access control is aimed to be achieved by identifying the individuals themselves, implemented using biometric identification technologies. One particular biometric identification technology used for people flow control uses face recognition to identify individuals. While face recognition technology has its merits, it is prone to error and is therefore often unreliable. Furthermore, face recognition technology has proven to be greatly affected by face covering, being for cultural and/or hygienic reasons. Further, face recognition is based on at least one camera which is always active which is not energy efficient. Alternative particular biometric identification technology used for access flow control uses fingerprint to identify individuals. Such is however disadvantageous as fingerprint recognition is often unreliable (slow, affected by the dryness of one's skin) and is particularly disadvantageous as it requires contact with a frequently used surface (the fingerprint reader).

[0004] According to a further known approach, referred to as "what you have", access control is based on identifying individuals using something the user possesses, referred to as a token or authentication medium. Particularly advantageous are keyless entry systems due to their convenience and/or reliability. Keyless entry systems may for example operate in that an BLE (Bluetooth Low Energy) or UWB (Ultra-Wideband) access control terminal executes a wireless communication with an authentication device, such as a keyless fob, a keycard or an authentication medium incorporating a corresponding wireless transceiver. Once said wireless communication between the access control terminal and the authentication medium has been executed, the access control terminal exchanges data messages with the authentication medium. The authentication can be initiated either by a user, for instance by pressing a button on the authentication medium to trigger transmission of authentication data to the access control terminal. Upon successful authentication, i.e. verification of user credentials (e.g. by correlating authentication data received from the authentication device with a list of authorized users), the access control terminal grants access to the user in possession of the respective authentication medium, e.g. by opening said barrier. On the other hand, if the authentication fails, the access control terminal denies access to the user in possession of the respective authentication medium, e.g. by locking the barrier/ by keeping the barrier locked.

[0005] For close-range applications, a radio-frequency identification (RFID) transponder (or tag) is often used, which has mostly replaced earlier magnetic stripe cards. Other current solutions use infra-red systems or radio systems to transmit an authenticating signal from an authentication medium to an access control terminal of a security control system. Close proximity keyless systems, (i.e. between direct contact and a threshold of a few centimeters), for example RFID based systems, allow determination of a user's proximity to a barrier by appropriate placement of a reader of the access control terminal. However, as their name implies close-proximity keyless systems suffer from the disadvantage that they require a very close proximity of the authentication medium to the access control terminal. In order to overcome this disadvantage, mid-range keyless entry systems have been proposed, in particular based on BLE and/or UWB communication. UWB systems are advantageous since they allow reliable mid-range communication without a user having to precisely identify the reader device. As the communicating range between an authentication device and an UWB access control terminal increases, the convenience and ease-of-use increases, because the authentication medium does not need to be placed in very close range, such as less than one centimeter from the UWB access control terminal. The user no longer needing to precisely locate the UWB access control terminal (or its antenna) not only adds convenience but also has the potential to speed up the process, thereby increasing the throughput through a barrier.

[0006] The network topologies of said access control systems typically comprise a central access rights server to which each access control terminal is connected. An authentication medium held by a user is brought close to an access control terminal for wireless exchange of credentials. These credentials are then transmitted from the access control terminal to the server, which performs a look-up in a database of access rights. If access is granted, the server sends a signal to the access control terminal, which allows the user access through an electronically controlled doorway. The disadvantage of this topology is that it requires each access control terminal to be permanently connected to the server, which is associated with considerable cost in wiring and presents a single point of failure. More modern access control systems have relegated access control decisions to the access control terminals themselves. If these access control terminals are not connected to the server, however, the issue then arises of how and when to update the database of access rights in each access control terminal.

[0007] Other access rights systems invert the situation by storing a database or table of the user's access rights in the mediums themselves. At an access control point, the access control terminals and the authentication medium exchange data containing an identifier of the access control terminal and the user's access rights at that access control point. Authentication mediums are however vulnerable entities with respect to date protection. Further, updating access rights becomes cumbersome as every affected party must have its authentication medium updated with new access rights.

[0008] Other solutions relate to access enforcement points that are configured to operate an access point, e.g. unlocking a door, and that constantly communicate with another device. Such access enforcement points may operate by a battery that has to be exchanged from time to time. Considering that an access enforcement point that constantly communicates with another device and/or searches for another device constantly consumes considerable amounts of energy, such a solution is not necessarily energy-efficient and further requires maintenance.

[0009] The article "Recognizing Hand Gestures using Solar Cells" by Dong Ma et al., IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2022.3148143 discloses a system which can recognize hand gestures near a solar-powered device by analyzing the patterns of the photocurrent.

[0010] None of the known concepts provides an energy-efficient and at the same time easy-to-use solution for a wakeup of access control points. Therefore, there is a need for such solution.

SUMMARY OF THE INVENTION

[0011] It is an object of the present invention is to provide a wakeup method for an access enforcement point which at least partially overcomes the above-mentioned disadvantages. In particular, it is an object of the present invention to provide a wakeup method which is energy-efficient and intuitive to use. According to the present invention, the above-mentioned objects are addressed through the features of the independent claims. In addition, further advantageous embodiments follow from the dependent claims and the description.

[0012] According to a first aspect of the present invention, a computer-implemented wakeup method is provided, which may be performed by an access enforcement point. The access enforcement point may be configured to cause operation, preferably unlocking and/or locking, of an access point. The access enforcement point may comprise energy harvesting means. The energy harvesting means may include a solar cell and an energy storage. The method may comprise harvesting light, e.g. ambient light, and generating, by the solar cell, a solar cell signal. The method may comprise determining that the solar cell signal satisfies a mode switching condition. The method may comprise, e.g. in response to determining that the solar cell signal satisfies a mode switching condition, switching the access enforcement point from a sleep mode into an active mode. The mode switching condition may comprises a drop of the solar cell signal that may correspond to a reduction of light, e.g. ambient light, incident on the solar cell that may occur upon, preferably manually, masking the solar cell, e.g. upon manually masking the solar cell partially.

[0013] The method may allow to wakeup an access enforcement point.

[0014] The wakeup method does not require using a dedicated switch that only serves for wakeup purposes. Instead, the solar cell, which is anyway used for energy harvesting, can be used. Thereby, the wakeup method allows for an easy and cost-efficient construction of access enforcement point, and for an easy and cost-efficient wakeup method.

[0015] Allowing the access enforcement point to be in a sleep mode allows for an energy-efficient access enforcement point. Thus, energy harvesting means need to provide less energy and may be manufactured more cost-efficient.

[0016] Allowing the access enforcement point to be in a sleep mode allows to reduce the energy consumption of the access enforcement point and thereby reduces the need of maintenance. In other words: An access enforcement that is configured to perform the above wakeup method essentially only needs maintenance in case it is damaged or in case it runs out of energy.

[0017] Considering that the access enforcement point may not be connected to a power grid and may instead by powered by its own energy harvesting means, e.g. powered completely by the energy harvesting means, it is desired to reduce the energy consumption of the access decision point, e.g. by only operating in an active mode when such an operation may be required, e.g. when an intent to operate the access point is likely and/or when an instruction is likely to be sent to the access enforcement point.

[0018] The active mode may be a mode in which the access enforcement point is able to cause operation of the access point. The active mode may be a mode in which the access enforcement mode is able to send an instruction request. The active mode may be a mode in which the access enforcement mode is able to receive an instruction.

[0019] The sleep mode may be a mode in which the access enforcement point is able to determine that the solar cell signal satisfies a mode switching condition. The sleep mode may be a mode in which the access enforcement point is able to harvest ambient light and generating, by the solar cell, a solar cell signal.

[0020] The sleep mode may be a mode, in which less energy is consumed by the access enforcement point as compared to the access enforcement point being in the active mode.

[0021] The term "the mode switching condition is based or comprises condition XYZ" may refer to that the mode switching condition is satisfied if condition XYZ is satisfied. The mode switching condition may comprise/may be based on more than condition, e.g. on conditions XYZ and ABC. In some embodiments, the mode switching condition may be satisfied if all conditions the mode switching condition is based on/comprises are satisfied, e.g. if both XYZ and ABC are satisfied. In some embodiments, the mode switching condition may be satisfied if at least one of the conditions the mode switching condition is based on/comprises is satisfied, e.g. if at least one of XYZ and ABC is satisfied.

[0022] The term access enforcement point may include any device that is capable of unlocking and/or locking an access point. In particular, the access enforcement point may not have decision taking capabilities for deciding whether to unlock or not based on the validity of a credential. Rather, the access enforcement point may be capable of performing or causing unlocking and/or locking a respective access point upon receiving a respective command. Each access enforcement point may be associated to/may have an access point. Each access point may be associated to/may have an access enforcement point. For example, the access enforcement point may include an actuator for unlocking and/or locking the access point. Thus, in other words, the access enforcement point may be understood as a stupid device which may only execute commands without taking any decision, e.g., on whether a user has an intent to unlock or whether the user is allowed to access a respective access point. Further, the access enforcement point may be capable of low-power wireless communication in order to receive said commands, in particular from one or more access decision points and/or from an authentication medium. Due to this configuration of the access enforcement point, the access enforcement point may be operated with a very low energy consumption. This is beneficial because the need for maintenance is significantly reduced. In other words: An access enforcement point essentially only needs maintenance in case if it is damaged or in case if it runs out of energy. The access enforcement point may not be connected to a power grid in order to keep the installation effort low.

[0023] The access enforcement point may be a low-power access enforcement point.

[0024] It may be provided that an access enforcement point causes unlocking of an associated access point e.g. upon receiving an unlock-command from an access decision point. The access enforcement point may therefore include means for performing/causing unlocking, e.g., a lock. The access enforcement point may be configured to cause operation of the access point, in particular unlocking and/or locking of the access point.

[0025] It may be provided that the access enforcement point and/or the access point include signaling means, in particular a visual signaling means and/or an acoustic signaling means , e.g. for indicating a status and/or an operation of the access enforcement point and/or the access point, e.g. locked/unlocked..

[0026] The method may comprise storing energy, e.g. electrical energy, generated by the solar cell, in the energy storage. The energy harvesting means and/or the energy storage may be adapted to provide an amount of energy to the access enforcement point that is sufficient to operate the access enforcement point. I.e., the energy harvesting means and/or the energy storage may be adapted to power the access enforcement point. The access enforcement point may not be electrically connected to a power-grid. The access enforcement point be electrically independent from a power-grid. The solar cell may be configured to charge the energy storage, i.e. to transfer energy into the energy storage. The energy storage may be configured to power the access enforcement point in the absence of a solar cell signal, e.g. in the dark.

[0027] The solar cell signal may be a time dependent signal. The solar cell signal may be a photocurrent and/or a photocurrent density, e.g. generated by the solar cell. The solar cell signal may be a current and/or a current density, e.g. generated by the solar cell. The solar cell signal may be a voltage, e.g. a voltage output by the solar cell. The solar cell signal may be filtered and/or averaged, e.g. averaged for a predetermined amount of time using a moving average. The solar cell signal may be amplified, e.g. by the access enforcement point. The access enforcement point may be configured to internally amplify the solar cell signal.

[0028] Switching the access enforcement point from a sleep mode into an active mode may be and/or may comprise a wakeup of the access enforcement point.

[0029] Switching the access enforcement point from a sleep mode into an active mode may be triggered when the mode switching condition is satisfied/met. The drop of the solar cell signal comprised in the mode switching condition may be an abrupt drop, i.e. it may be a sudden drop and/or it may be drop by a predetermined extent, e.g. a large extent. The predetermined extent may be an extent relative to the solar cell signal, e.g. 25 % or more, 50 % or more or 75% or more. The predetermined extent may be an absolute extent.

[0030] Ambient light may be light from indoor lighting and/or may be indoor light and/or may be sunlight, e.g. sunlight passing through windows in a building. Ambient light may be light from windows.

[0031] The solar cell may be an indoor solar cell. The area of the light-receiving surface of the solar cell may be less than 100 cm^2, or less than 50 cm^2. The area of the light-receiving surface of the solar cell may be smaller than the average palm of a human hand. The area of the light-receiving surface of the solar cell may be smaller than the average area of a physical keycard.

[0032] Masking the solar cell may refer to masking the solar cell surface.

[0033] The mode switching condition may comprises a drop of the solar cell signal that may correspond to a reduction of ambient light incident on the solar cell that may occur upon manually masking the solar cell, e.g. masking more than 10 % of the solar cell surface and/or masking more than 25 % of the solar cell surface and/or masking more than 50% of the solar cell surface and/or masking more than 75 % of the solar cell surface. The solar cell does not need to be entirely masked/covered. The solar cell may be partially masked/covered. The term masking may correspond to covering. When manually masking the solar cell, the fingers may be spread. Masking only a percentage of the solar cell may be referred to as partially masking the solar cell and/or may be referred to as masking the solar cell.

[0034] If in doubt, it may be better to switch the access enforcement point too often into an active mode, as compared to risking not switching into an active mode when switching into an active mode is desired, e.g. desired by a user.

[0035] The solar cell may be manually masked by a user such that essentially no ambient light is incident on the solar cell, e.g. more than 90% of the solar cell surface may be masked.

[0036] The solar cell e.g. may be masked by a physical keycard. E.g., the access enforcement point may comprise a keycard reader, and masking the solar cell by the keycard may at the same time allow to read out the keycard and/or to receive a credential from the keycard. The keycard may be an authentication medium.

[0037] The drop of the solar cell signal, e.g. the fraction by which the solar cell signal drops, may correspond to the fraction of the solar cell surface that is masked, e.g. manually masked.

[0038] It may be provided that the access point is a postbox and/or a parcel box and/or a door and/or a lockable piece of furniture and/or an access restricted trigger mechanism. An access restricted trigger mechanism may be provided at an elevator, wherein unlocking the access restricted trigger mechanism causes the elevator to perform a predetermined action, e.g., moving to a specific floor or locking the elevator while keeping the elevator door open.

[0039] The access enforcement point may comprise a wakeup sensor which may be used by a user in order to cause the access enforcement point to, preferably immediately, switch from a sleep mode into an active mode. The solar cell may be used as a wakeup sensor, in particular wherein the user may cover the solar cell, e.g., by his hand or body, causing a sudden drop in the amount of incident light which may be interpreted as a wakeup signal.

[0040] The method may further comprise, e.g. upon switching the access enforcement point into an active mode, sending, by the access enforcement point, an instruction request.

[0041] A timing of sending the instruction request may be set based on switching the access enforcement point into the active mode. Sending an instruction request by the access enforcement point may be triggered by/upon switching the access enforcement point in an active mode.

[0042] Sending, by the access enforcement point, may comprise broadcasting and/or polling and/or repeatedly sending and/or multicasting. The access enforcement point may send the instruction request to multiple access decision points and/or may be configured to send the instruction request to multiple access decision points. Sending may be done in a broadcasting manner. The instruction request may be a broadcasting signal.

[0043] The access enforcement point may send the instruction request to multiple devices and/or may be configured to send the instruction request to multiple devices, e.g. devices other than access enforcement points.

[0044] Sending the instruction request upon switching into an active mode allows to send instruction requests once there is a high likelihood that a user intends to operate the access point. Sending the instruction request upon switching into an active mode, e.g. upon determining that a solar cell signal satisfies a mode switching condition, may allow to reduce the probability/rate of sending instruction requests when there is not intention to operate the access point. Thus, the energy consumption of the access enforcement point may be reduced.

[0045] The method may further comprise receiving, by the access enforcement point, e.g. being in the active mode, an instruction, preferably in response to sending the instruction request. The instruction may include an operation-command to cause operation of the access point, e.g. an unlocking-command or a locking command. The method may further comprise causing, by the access enforcement point, operation of the access point according to the instruction, e.g. unlocking and/or locking.

[0046] The operation may be an unlocking operation and/or a locking operation. There may be a plurality of access enforcement points and a plurality of access points. Each access point may have an access enforcement point configured to cause operation of the respective access point.

[0047] The instruction request may be received by the access enforcement point without having sent a respective instruction request by the access enforcement point. The sender of an instruction may be connected to a power grid and/or may have an own energy storage that is independent from the energy storage of the access enforcement point. E.g., an access decision point may send the instruction, and/or an authentication medium may send the instruction.

[0048] Sending instructions that may not be received by the access enforcement point, e.g. due to the access enforcement point being in the inactive mode, is not detrimental to the energy consumption of the access enforcement point. On the other side, it may be detrimental for the access enforcement, e.g. being powered by its own energy harvesting means, in terms of the energy consumption of the access enforcement point, to be in active mode, when there is no intent to operate an access point and/or when no instruction is likely to be received by the access enforcement point.

[0049] The instruction may be received from an authentication medium, preferably a mobile device or a physical keycard. The instruction may include a credential. In some embodiments of the present invention, a validity of the credential may be determined prior to causing operation of the access point and operation of the access point may only be caused upon determining that the credential is valid. In some embodiments of the present invention, the instruction may include a command to cause operation of the access point independent of a validity of the credential and/or of the instruction. In some embodiments of the present invention, the instruction may include a command to cause operation of the access point without determining a validity of the credential and/or of the instruction.

[0050] The authentication medium e.g. may be a mobile device or a physical keycard. Operating the access point may comprise unlocking and/or locking the access point. The authentication medium may be configured to send an instruction.

[0051] The authentication medium may be a token, a badge, a mobile device, the user's body or a part of a user's body, e.g., being suitable for biometric detection, or the like. In case if the authentication medium is a user's body or a part of a user's body, an access decision point may perform camera tracking in order to determine whether the user intends to unlock a respective access point. Further, an access decision point may perform biometric authentication in order to check whether a respective user is allowed to access a respective access point. Biometric authentication may include for example face recognition, iris recognition or the like.

[0052] E.g. if the authentication medium is a token, badge or mobile device, the communication between the access enforcement point or the access decision point and the authentication medium may be performed wirelessly. In particular, the communication may include ultra-wideband transmissions and/or Bluetooth transmissions.

[0053] The validity of the credential may be determined using the authentication medium, e.g. by using a finger print sensor, e.g. of a smartphone, and/or by unlocking a lock screen.

[0054] The presence of a valid credential may be interpreted as a strong intent. Depending on the implementation of the present invention, an intent and/or a strong intent may be required.

[0055] It may be provided that the validity of the credential to unlock the respective access enforcement point is verified by a backend server with which e.g. an access decision point and/or the authentication medium may communicate.

[0056] The instruction may be received from an access decision point. The access decision point may be configured to receive the instruction request sent by the access enforcement point. The access decision point may be configured to receive a signal of an authentication medium of a user. The access decision point may be configured to determine an intent of the user to operate the access point, e.g. upon receiving the signal of the authentication medium. The access decision point may be configured to generate the instruction dedicated to the access enforcement point, e.g. upon determining the intent of the user. The access decision point may be configured to send the instruction to the access enforcement point, e.g. upon receiving the instruction request.

[0057] The term access decision point may include any kind of access controller which is capable to decide whether an access point should be unlocked or not. It may be capable of determining an intent to unlock an access point. Further, it may be capable of checking the validity of a user's credential. An access decision point may comprise an integrated and/or spaced apart tracking system which is capable of tracking a position of a user's authentication medium. Examples for said tracking systems are camera tracking systems and/or ultra-wideband tracking systems. In case if the access decision point comprises an ultra-wideband tracking system, the ultra-wideband tracking system may include a plurality of ultra-wideband anchors facilitating ranging of the authentication medium, in particular to determine successive positions of the authentication medium. Thus, an access decision point according to embodiments of the present invention may include an identification module which may be configured to verify a credential and/or an intent detection module which may for example track the user as described above, e.g. in order to determine the user's intent to access. The modules may be arranged spaced apart from each other and communicating with each other.

[0058] The access decision point may be connected to a power grid and/or may comprise a battery which is regularly to be replaced in order to prevent the access decision point from running out of energy. In a particular embodiment, the access decision point may be connected to a power grid and additionally comprise a battery in order to buffer potential blackouts in the power grid. An access control system then advantageously is capable of temporarily work during a blackout of a power grid.

[0059] The access decision point may be configured to communicate wirelessly with the access enforcement point. An access control system may include more than one access decision point and e.g. a plurality of access enforcement point. The number of access enforcement points comprised in the access control system may be larger than the number of access decision points comprised in the access control system.

[0060] The communication between the access enforcement point and the access decision point e.g. may be performed wirelessly via a low power communication protocol, such as Bluetooth Low Energy (BLE) or any other suitable low power communication protocols. The sending an instruction request by the access enforcement points therefore may be for example an advertising signal via Bluetooth.

[0061] The access decision point may be configured to determine an intent of the user, e.g. to determine an intent of the user upon receiving the signal of the authentication medium and/or e.g. upon receiving an instruction request. The access decision point may be configured to generate the instruction before receiving the instruction request, e.g. upon determining the intent of the user. The access decision point may be configured to send the instruction for a predetermined time period, e.g. at least 30 s, at least 1 min, at least 1.5 min, at least 2 min, or at least 5 min. Once the access enforcement point may have switched into the active mode, the access enforcement point may receive the instruction. In other words: The instruction may be sent from the access decision point during a predetermined period of time, during which the access enforcement point may be in a sleep mode first and later on in an active mode.

[0062] The access decision point may be connected to a power grid. Thus, sending instructions by the access decision point may not be energy-critical. Sending the instruction for a predetermined time period may enable the access enforcement point to receive an instruction immediately after switching into the active mode. It may also remove the need to send an instruction request by the access enforcement point. Thus, sending the instruction for a predetermined time period may allow to reduce the energy consumption by the access enforcement point.

[0063] The access decision point may be configured to send an instruction comprising a no-action command, e.g. if no intent of a user is determined and/or no signal of an authentication medium of a user is received and/or no instruction request is received from an access decision point. Sending an instruction comprising a no-action command may comprise not sending any instruction, i.e. the access enforcement point may be configured to interpret an absence of a received instruction, e.g. after having sent an instruction request, as a no-action command/a no-action instruction.

[0064] In some embodiments, the method may comprise: Determining, by the access enforcement point being in the active mode, that no instruction is received, e.g. within a predetermined time interval, from an access decision point, and sending an instruction request in response to determining that no instruction is received from an access decision point. Determining that no instruction is received may be performed in response to switching the access enforcement point into an active mode.

[0065] The computer-implemented wakeup method may be performed by an access control system. The access control system may include the access enforcement point, the access decision point, the access point and the energy harvesting means.

[0066] The access decision point may be configured to receive a credential, preferably from an authentication medium. The access decision point may be configured to determine a validity of the credential. Determining the validity of the credential preferably may be included in determining the intent of the user to operate the access point. In some embodiments, the access decision point preferably may be configured to only generate and/or send the instruction if the credential is determined to be valid.

[0067] The access decision point may be configured to receive the credential, preferably by receiving a signal from an authentication medium, wherein the signal comprises the credential.

[0068] The method may further comprise: upon receiving the instruction and/or after causing operation of the access point, switching the access enforcement point from the active mode to the sleep mode. The method preferably may further comprise a dead time after switching the access enforcement point from the active mode to the sleep mode. During the dead time, switching from the sleep mode to the active mode may be prevented and/or excluded.

[0069] The method may further comprise: upon switching into the active mode and not receiving an instruction for a predetermined period of time, switching the access enforcement point from the active mode to the sleep mode.

[0070] The method may further comprise: upon causing unlocking or locking of the access point, switching the access enforcement point from the active mode to the sleep mode. The method may further comprise: Not switching the access enforcement point into the sleep mode upon receiving a no-action command and/or not switching the access enforcement point into the sleep mode upon receiving a no-action command for a predetermined waiting time and then switching the access enforcement point into the sleep mode, e.g. if no instruction was received during the waiting time. The dead time may be a predetermined amount of time.

[0071] The method may further comprise, during a dead time after switching the access enforcement point from the active mode to the sleep mode, preventing and/or excluding switching from the sleep mode to the active mode.

[0072] It may be unlikely that an access point is operated twice within short time intervals, e.g. within a few seconds and/or minutes, e.g. during the night. For example, during night times it may be possible that only a security guard may pass an access point once every hour or every two hours. Thus, the dead time may allow a more energy-efficient operation of the wakeup method, while still allowing operation of the access point when desired by an authorized user. The dead time e.g. may be 10 s or less, 20 s or less, 30 s or less, 1 min or less, 2 min or less, or 5 min or less. The waiting time e.g. may be 10 s or less, 20 s or less, 30 s or less, 1 min or less, 2 min or less, or 5 min or less.

[0073] The dead time may allow also allow to prevent frequent switching into the active mode, e.g. when the mode switching condition is satisfied but there is in fact no intention to operate the access point.

[0074] The mode switching condition may be based on the signal of the solar cell dropping below a first solar cell dropping threshold and/or dropping by a second solar cell dropping threshold.

[0075] The second solar cell dropping threshold may be a threshold referring to an extent of a drop of the solar cell signal.

[0076] The first solar cell dropping threshold and/or the second solar cell dropping threshold may be predetermined. The first solar cell dropping threshold and/or the second solar cell dropping threshold may be absolute thresholds and/or relative thresholds, e.g. relative to a solar cell signal at a time before the solar cell signal satisfies the mode switching condition, and/or relative to a moving average of the solar cell signal. E.g., the mode switching condition may correspond to the solar cell signal dropping by 20% or more of the moving average of the solar cell signal over the past 10 s or less, past 30 s or less, past 1 min or less, and/or the solar cell signal dropping below e.g. 80% of the moving average of the solar cell signal. E.g., the mode switching condition may correspond to the solar cell signal dropping by 50% or more, or 75% or more, of the moving average of the solar cell signal over the past 10 s or less, past 30 s or less, past 1 min or less, and/or the solar cell signal dropping below e.g. 50% or less, or 25% or less of the moving average of the solar cell signal. The mode switching condition may be based on the signal of the solar cell being below a first solar cell dropping threshold. Relative thresholds may be dynamic/situation dependent thresholds.

[0077] The first solar cell dropping threshold and/or the second solar cell dropping threshold may be thresholds combining an absolute and a relative threshold, e.g. being below 80% of a moving average and being below a certain number of mA.

[0078] Using the first and/or the second solar cell dropping threshold may allow a robust and simple determination of whether the mode switching condition is satisfied. Using the first and/or the second solar cell dropping threshold may allow to avoid/reduce unnecessary switching into an active mode, e.g. erroneous/unintended switching.

[0079] The mode switching condition may be based on the signal of the solar cell exceeding a first solar cell threshold and/or being above a first solar cell threshold. The mode switching condition may be based on the signal of the solar cell dropping below/being below a second solar cell threshold. The mode switching condition may be based on the signal of the solar cell changing by a solar cell changing threshold. The mode switching condition may be based on the signal of the solar cell having a standard deviation being above/exceeding a standard deviation threshold.

[0080] The first solar cell threshold, the second solar cell threshold and the solar cell changing threshold may be predetermined thresholds, e.g. absolute and/or relative, e.g. in relation to a moving average of a solar cell signal.

[0081] The mode switching condition may be based on the signal of the solar cell first being above a first solar cell threshold and then being below a second solar cell threshold, and vice versa. The second solar cell threshold may be lower than the first solar cell threshold. This may provide a particularly robust switching condition, which reduces the rate/probability of erroneous/unintended switchings.

[0082] The signal of the solar cell may have a higher standard deviation e.g. if someone is approaching the solar cell. Having the mode switching condition being based on a standard deviation of the solar cell signal may allow faster mode switching of the access enforcement point, i.e. may reduce the latency between an intention to perform mode switching by the access enforcement point and actually performing mode switching by the access enforcement point. Having the mode switching condition being based on a standard deviation of the solar cell signal may allow faster operation of the access point, i.e. may reduce the latency between an intention to operate an access point and actually operating the access point. The standard deviation of the solar cell signal may be determined across a predetermined amount of time, e.g. 5 s or less, 10 s or less, 20 s less, or 30 s or less.

[0083] A change of the solar cell signal within a tolerance range, e.g. a change being lower than a changing threshold, may be disregarded for determining whether the switching condition is met. The tolerance range/the changing threshold may be defined such that people moving near the access enforcement point causing a change of the amount of incident light may be disregarded, i.e., do not trigger a wakeup. This may allow to reduce the rate of unintentionally switching the access enforcement point into an active mode, which in turn may reduce the energy consumption of the access enforcement point.

[0084] The mode switching condition may be based on a solar cell signal at a first time being above the first solar cell threshold and a solar cell signal at a second time being below the second solar cell threshold, or a solar cell signal at a first time being below the second solar cell threshold and a solar cell signal at a second time being above the first solar cell threshold. The second time may be later than the first time and the time difference between the first time and the second time may be 100 ms or less, 500 ms or less, 1 s or less, or 2 s less. The solar cell signal at the first time and the solar cell signal at the second time may be respectively averaged for a predetermined amount of time.

[0085] The solar cell signal being above the first solar cell threshold at a first time and being below a second solar cell threshold at a second time may correspond e.g. to a drop of the solar cell signal corresponding to a reduction of ambient light incident on the solar cell that may occur upon manually masking the solar cell.

[0086] The solar cell signal being below the second solar cell threshold at a first time and being above a first solar cell threshold at a second time may correspond to an increase of the solar cell signal corresponding e.g. to an increase of ambient light incident on the solar cell that may occur e.g. when a lighting in a building is turned on and/or when the solar cell is deliberately irradiated.

[0087] The solar cell signals at the first and the second time may be measured and e.g. averaged.

[0088] The second solar cell threshold may be at least one of the following: a value calibrated during operation of the solar cell, a design value of the solar cell, a fraction of a moving average of a solar cell signal, averaged across a predetermined amount of time, in particular for the past 100 ms or less, 250 ms or less, 500 ms or less, 1 s or less, 5 s or less, 10 s or less, 30 s or less, 1 min or less, 2 min or less, 5 min or less, or 10 min or less, a fraction of an average solar cell signal, averaged across 24 hours, a fraction of a value corresponding to a solar cell signal at typical ambient light at the location of the solar cell, preferably when lighting is turned on, a fraction of a value corresponding to a solar cell signal at an irradiation strength of AM1.5, or AM2, AM5, or AM10, or a photocurrent density of below 1 mA/cm^2, preferably below 500 μA/cm^2, more preferably below 100 μA/cm^2, even more preferably below 50 μA/cm^2.

[0089] The first solar cell threshold may be at least one of the following: a value calibrated during operation of the solar cell, a design value of the solar cell, a multiple of a moving average of a solar cell signal, averaged across a predetermined amount of time, in particular for the past 100 ms or less, 250 ms or less, 500 ms or less, 1 s or less, 5 s or less, 10 s or less, 30 s or less, 1 min or less, 2 min or less, 5 min or less, or 10 min or less, a multiple of an average solar cell signal, averaged across 24 hours, a multiple of a value corresponding to a solar cell signal at typical ambient light at the location of the solar cell, preferably when lighting is turned on, a multiple of a value corresponding to a solar cell signal at an irradiation strength of AM1.5, or AM2, AM5, or AM10, a photocurrent density of above 100 μA/cm^2, preferably above 500 μA/cm^2, more preferably above 1 mA/cm^2.

[0090] Using thresholds referring to the solar cell signal may provide particularly robust switching conditions, which reduce the rate/probability of erroneous/unintended switching operations.

[0091] Thresholds referring to the solar cell signal may be calibrated during operation of the solar cell. E.g., the thresholds may be calibrated individually for each solar cell. Common thresholds for a plurality of solar cells that are calibrated based on the plurality of the solar cells may also be used. Calibration may be done under typical operating conditions, i.e. when the solar cell is at the typical location of operation, and under typical ambient light conditions.

[0092] Thresholds referring to the solar cell signal may be based on design values provided by the manufacturer of the solar cell.

[0093] Thresholds referring to the solar cell signal may be based on fractions of averaged solar cell signals. The term fraction may refer to factors of solar cell signals, wherein the factors may be smaller than one, e.g. 75 % or less, 50 % or less, 25 % or less, or 10% or less.

[0094] Thresholds referring to the solar cell signal may be based on multiples of averaged solar cell signals, wherein the multiples may be larger than 1, e.g. 1.25 or more, 1.5 or more, 2 or more, 3 or more, or 5 or more.

[0095] Thresholds referring to the solar cell signal may be based on averaged solar cell signals which are averaged over a predetermined amount of time, e.g. 1 min or less, 2 min or less, 5 min or less, 10 min or less, or 24 h or less, e.g. in the typical location of the solar cell, e.g. under typical ambient light conditions.

[0096] The term irradiation strength of AMX, X being number, refers to the air mass, as is known to the skilled person.

[0097] The mode switching condition may be adjusted depending on the solar cell signal. The first solar cell dropping threshold and/or the second solar cell dropping threshold may be adjusted based on the solar cell signal at a time before the solar cell signal satisfies the mode switching condition.

[0098] The mode switching condition may be based on the solar cell signal. The mode switching condition may depend on the solar cell signal. The mode switching condition may be set/adjusted based on the solar cell signal.

[0099] The first solar cell dropping threshold and/or the second solar cell dropping threshold may be adjusted based on the solar cell signal at a time before determining that the solar cell signal satisfies the mode switching condition.

[0100] E.g., if the ambient light is bright, the first solar cell dropping threshold may be much lower as compared to unaffected signal, i.e. the signal before the solar cell is masked. E.g., if the ambient light is dark, i.e. if there is not much ambient light, the first solar cell dropping threshold may be only a bit lower as compared to unaffected signal, i.e. the signal before the solar cell is masked.

[0101] The mode switching condition may depend on an energy storage level of energy stored in the energy storage. The mode switching condition may be adjusted depending on the energy storage level. The mode switching condition may be relaxed at a higher energy storage level and/or tightened at a lower energy storage level.

[0102] Relaxing the mode switching condition at higher energy storage levels may allow to reduce the probability of false negative errors, i.e. the probability for not switching into an active mode even though switching is desired.

[0103] Tightening the mode switching condition at lower energy storage levels may allow to keep the access enforcement point functional, i.e. to avoid that the energy storage level is running out of stored energy.

[0104] Tightening the mode switching condition e.g. may comprise decreasing the first solar cell dropping threshold and/or increasing the second solar cell dropping threshold. Relaxing the mode switching condition e.g. may comprise increasing the first solar cell dropping threshold and/or decreasing the second solar cell dropping threshold.

[0105] It is less likely to determine that a tighter mode switching condition is satisfied as compared to a more relaxed mode switching condition. In other words: Certain solar cell signals may not satisfy a tight mode switching condition but may satisfy a relaxed mode switching condition.

[0106] The mode switching condition may be dynamically adjusted depending on the energy storage level. The mode switching condition may be dynamically adjusted in discrete steps depending on the energy storage level, i.e. there may be several discrete mode switching conditions. The mode switching condition may be dynamically adjusted continuously depending on the energy storage level. The mode switching condition may be dynamically adjusted such that the energy storage level is kept within a predetermined range.

[0107] The method may further comprise charging the energy storage, using the solar cell, wherein the solar cell may be deliberately irradiated using a light source, e.g. by a user, e.g. using an external light source. The mode switching condition may be based on the charging, preferably based on the solar cell signal exceeding a charging solar cell threshold and/or based on the energy storage exceeding an energy storage threshold.

[0108] Charging the energy storage may comprise/may be understood as transferring energy to the energy storage. The method may comprise charging the energy storage by deliberately irradiating the solar cell, e.g. by a user, using a light source, e.g. an external light source.

[0109] The charging solar cell threshold may be a predetermined threshold. The charging solar cell threshold may be an absolute threshold and/or a relative threshold, e.g. relative to a solar cell signal at a time before the solar cell signal exceeds the charging solar cell threshold and/or relative to a moving average of the solar cell signal. E.g., the charging solar cell threshold may correspond to 120% or more of the moving average of the solar cell signal over the past 10 s or less, past 30 s or less, past 1 min or less, or 150% or more, or 200% or more.

[0110] The energy storage threshold may be at least 100 % or less, or 125 % or less, or 150 % or less, or 200 % or less, of a total amount of energy, required by the access enforcement point to determine that a signal of the solar cell corresponds to a mode switching condition for a predetermined integer number of times, to switch the access enforcement point from a sleep mode into an active mode for a predetermined integer number of times and to cause operation of the access point according to the instruction once or for a predetermined integer number of times, and preferably to receive an instruction for the predetermined integer number of times, and more preferably to send an instruction request for the predetermined integer number of times. The predetermined integer number e.g. may be 1, or 2, or 3, or 4, or 5.

[0111] The energy storage threshold may prevent switching the access enforcement point into an active mode when there is not enough energy in the energy storage to perform desired actions by the access enforcement point.

[0112] The charging solar cell threshold may allow to determine that the energy storage of the access enforcement point is deliberately charged.

[0113] The charging solar cell threshold and/or the energy storage threshold may allow to operate/to use an access enforcement point even when the energy storage of the access enforcement point is empty or nearly empty.

[0114] The mode switching condition may be based on a level of energy stored in the energy storage being below the energy storage threshold. Preferably, the energy storage threshold may be at least a total amount of energy required by the access enforcement point to determine that a signal of the solar cell corresponds to a mode switching condition for a predetermined integer number of times, to switch the access enforcement point from a sleep mode into an active mode for a predetermined integer number of times and preferably to cause operation of the access point according to the instruction once or for a predetermined integer number of times, and preferably to receive an instruction for the predetermined integer number of times, and more preferably to send an instruction request for the predetermined integer number of times, wherein the predetermined integer number may e.g. be 1, or 2, or 3, or 4, or 5.

[0115] The energy storage threshold may relate to a minimum amount of energy stored in the energy storage threshold that is required for the access enforcement point to be able to perform the essential operations. If the level of energy stored in the energy storage is close to the energy storage threshold, e.g. being only 125% or less of the energy threshold, or even below, the mode switching condition may be made very strict, in order to minimize the risk/rate for an unintentional/erroneous mode switching as much as possible, and in order to still enable a useful operation of the access enforcement point even at such a low energy storage level.

[0116] According to a second aspect of the present invention, a use of an access enforcement point in a computer-implemented wakeup method according to the first aspect of the present invention may be provided. The access enforcement point may include: energy harvesting means comprising an energy storage and a solar cell, a communication interface, preferably for communicating with an access decision point and/or with an authentication medium, preferably means for causing operation of an access point; and processing means for determining that a signal of the solar cell corresponds to a mode switching condition and for switching the access enforcement point from a sleep mode into an active mode.

[0117] According to a third aspect of the present invention, an access enforcement point may be provided. The access enforcement point may comprise energy harvesting means, and the energy harvesting means may comprise an energy storage and a solar cell. The access enforcement point may be adapted/may be configured to perform the following actions: determine that a signal of the solar cell satisfies a mode switching condition, switch the access enforcement point from a sleep mode into an active mode, e.g. in response to determining that a signal of the solar cell satisfies a mode switching condition, and preferably cause operation of an access point. The access enforcement point may be configured to be used in a computer-implemented wakeup method according to the first aspect of the present invention.

[0118] According to a fourth aspect of the present invention, an access control system may be provided. The access control system may comprise at least one access enforcement point and at least one an access point. One of the at least one access enforcement points may comprise energy harvesting means that may include a solar cell and an energy storage. The access control system may be configured to perform a computer-implemented wakeup method according to the first aspect of the present invention.

[0119] According to a fifth aspect of the present invention, a computer program or a computer-readable medium may be provided, comprising computer-readable instructions which when executed by a data processing system cause the data processing system to perform the computer-implemented wakeup method according to the first aspect of the present invention.

[0120] All technical implementation details and advantages described with respect to the first aspect of the present invention are self-evidently mutatis mutandis applicable for the second, third, fourth and fifth aspects of the present invention and vice versa.

[0121] The terms "plurality" and "more than one" may be used interchangeably unless otherwise specified. The terms "locking/unlocking" and "operation/operating" may be used interchangeably unless otherwise specified. The terms "at least one" and "one or more" include the term "plurality". The terms "plurality" and "more than one" may be used interchangeably unless otherwise specified.

BRIEF DESCRIPTION OF THE DRAWINGS

[0122] The present invention will be explained in more detail, by way of example, with reference to the drawings in which:

Figure 1 is a highly schematic perspective view of an access enforcement point and a user according to embodiments of the present invention.

Figure 2 is a high-level flow chart diagram illustrating a first sequence of a wakeup method according to embodiments of the present invention.

Figure 3A is an illustrative example of a drop of a solar cell signal corresponding to a reduction of ambient light incident on the solar cell that may occur upon manually masking the solar cell.

Figure 3B is another illustrative example of a drop of a solar cell signal corresponding to a reduction of ambient light incident on the solar cell that may occur upon manually masking the solar cell.

Figure 3C is an illustrative example of an increase of a solar cell signal corresponding to an increase of ambient light incident on the solar cell that may occur upon switching lightings in a building on.

Figure 4 is a schematic perspective view of a building comprising an access control system comprising access enforcement points that implement a wakeup method according to embodiments of the present invention.

FIGURATIVE DESCRIPTION OF EMBODIMENTS

[0123] Figure 1 is a highly schematic perspective view of an access enforcement point and one user according to embodiments of the present invention. The access enforcement point 201 is configured to cause operation of the access point 201a. The access enforcement point 201 comprises energy harvesting means comprising a solar cell (not shown) and an energy storage (not shown), e.g. a battery.

[0124] The user 301 may approach the access enforcement point 201. The user 301 may cause a drop of the solar cell signal by manually masking the solar cell surface. The access enforcement point 201 may determine that the solar cell signal satisfies a mode switching condition, which may comprise a drop of the solar cell signal, e.g. corresponding to a reduction of ambient light incident on the solar cell. The access enforcement point 201 may, e.g. in response to determining that the solar cell signal satisfies the mode switching condition, switch from a sleep mode into an active mode.

[0125] The user 301 has an authentication medium 301a which may carry a valid credential for the access point 201a. The authentication medium 301a may send an instruction to the access enforcement point 201. The instruction may include the credential. In some embodiments, a validity of the credential may be determined and operation of the access point may only be caused upon determining that the credential is valid. In some embodiments, the instruction may include a command to cause operation of the access point 201a independent of determining a validity of the credential and/or the instruction.

[0126] An access decision point 101 (not shown) may communicate with the authentication medium 301a and may determine an intent of the user 301 to operate/cause operation of the access point 201a. For example, the intent determination may be carried out based on successive positions or a moving direction and/or speed of the authentication medium 301a. Alternatively or in addition, the intent may be determined based on the validity of the credential. This scenario set forward, the following may happen: The next time the access decision point 101 receives an instruction request from the access enforcement point 201, it may respond an unlock-command causing the access enforcement point 201 to unlock the access point 201a such that the user 301 can access the access point 201a.

[0127] The access enforcement point 201 may be in an active mode. The access enforcement point 201, e.g. being in an active mode, may communicate with the authentication medium 301a and may receive an instruction by the authentication medium 301a of the user 301 to operate/cause operation of the access point 201a. The access enforcement point 201 may cause operation of the access point 201a, e.g. upon receiving the instruction.

[0128] Fig. 2 is a high-level flow chart diagram illustrating a first sequence of a wakeup method according to embodiments of the present invention. The method includes step S01 of harvesting ambient light and generating a solar cell signal, step S02 of determining that the solar cell signal satisfies a mode switching condition, and step S03 of switching the access enforcement point into an active mode. Optional step S04 includes sending an instruction request. Optional step S05 includes receiving an instruction request. An instruction request may be received without having send an instruction request beforehand. Optional step S06 includes causing operation of the access point according to the instruction.

[0129] Figure 3A is an illustrative example of a drop of a solar cell signal corresponding to a reduction of ambient light incident on the solar cell that may occur upon manually masking the solar cell. A threshold, e.g. a first solar cell dropping threshold, is indicated by the dotted line. The units of the solar cell signal and the time are arbitrary units (a.u.) respectively, and may e.g. be linear units or logarithmic units.

[0130] Figure 3B is an illustrative example of a drop of a solar cell signal corresponding to a reduction of ambient light incident on the solar cell that may occur upon manually masking the solar cell. Here, a standard deviation of the solar signal increases before the solar cell signal drops. The increased standard deviation may be caused by / related to a user approaching the solar cell.

[0131] Figure 3C is an illustrative example of an increase of a solar cell signal corresponding to an increase of ambient light incident on the solar cell that may occur upon turning a lighting in a building on and/or when the solar cell is deliberately irradiated. A dashed-dotted line indicates a threshold, e.g. a charging solar cell threshold.

[0132] Figure 4 is a schematic perspective view of a building comprising an access control system comprising access enforcement points that may implement a wake-up method according to embodiments of the present invention.

[0133] In the description of Figure 4, the reference signs 101, 102, 103, 104, 105, 106, 107, 108 are abbreviated as 101, ..., 108; the reference signs 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212 are abbreviated as 201, ..., 212; the reference signs 201a, 202a, 203a, 204a, 205a, 206a, 207a, 208a, 209a, 210a, 211a, 212a are abbreviated as 201a, ..., 212a; the reference signs 301, 302, 303, 304 are abbreviated as 301, ..., 304; and the reference signs 301a, 302a, 303a, 304a are abbreviated as 301a, ..., 304a.

[0134] The building comprises a plurality of access points 201a, ..., 212a. Each access point 201a, ..., 212a has a respective access enforcement point 201, ..., 212 which includes, in the illustrated example of figure 4, an actuator in the door leaf which is capable to unlock and/or lock the access point 201a, ..., 212a. Further, the building is equipped with a plurality of access decision points 101, ..., 108 which are distributed throughout the building. The access enforcement points 201, ..., 212 may send instruction requests to the access decision points 101, ..., 108, e.g. upon switching into an active mode. The instruction requests may be received by at least part of the access decision points 101, ..., 108, e.g., by the access decision points 101, ..., 108 which are in wireless communication range of a respective access enforcement point 201, ..., 212.

[0135] As it is depicted in figure 4, a plurality of users 301, ..., 304 are in and near the building. Each user 301, ..., 304 has a respective authentication medium 301a, ..., 304a. The authentication mediums 301a, ..., 304a, according to the illustration of figure 4, are mobile devices capable of communicating wirelessly. If one access decision point 101, ..., 108 receives a signal from an authentication medium 301a, ..., 304a of a user 301, ..., 304, which may be a mobile device, and determines an intent of the user 301, ..., 304 to unlock a respective access enforcement point 201, ..., 212, the access decision point 101, ..., 108 may generate an instruction and may send it to the respective access enforcement point 201, ..., 212, e.g. in response to receiving an instruction request from the respective access enforcement point 201, ..., 212. In some embodiments, generating the instruction may be only performed, if in addition to the intent, a valid credential is successfully validated by the access decision point 201, ..., 212. The respective instruction may include an unlock-command causing the respective access enforcement point 201, ..., 212 to unlock. Hence, the user 301, ..., 304 may be able to access the respective access point 201a, ..., 212a. If no intent to unlock or no valid credential is received/determined by the access decision point 201, ..., 212, the instruction may be a no-action command. The no-action command may be also seen in undertaking no action, i.e., not responding at all.

[0136] Although some aspects have been described in the context of an apparatus, it is clear that these aspects also represent a description of the corresponding method, where a block or device corresponds to a method step or a feature of a method step. Analogously, aspects described in the context of a method step also represent a description of a corresponding block or item or feature of a corresponding apparatus.

[0137] Some or all of the method steps may be executed by (or using) a hardware apparatus, such as a processor, a microprocessor, a programmable computer or an electronic circuit. Depending on certain implementation requirements, embodiments of the invention can be implemented in hardware or in software. The implementation can be performed using a non-transitory storage medium such as a digital storage medium, for example a floppy disc, a DVD, a Blu-Ray, a CD, a ROM, a PROM, and EPROM, an EEPROM or a FLASH memory, having electronically readable control signals stored thereon, which cooperate (or are capable of cooperating) with a programmable computer system such that the respective method is performed. Therefore, the digital storage medium may be computer readable.

[0138] Some embodiments of the invention provide a data carrier having electronically readable control signals, which are capable of cooperating with a programmable computer system, such that one of the methods described herein is performed.

[0139] Generally, embodiments of the invention can be implemented as a computer program (product) with a program code, the program code being operative for performing one of the methods when the computer program product runs on a computer. The program code may, for example, be stored on a machine-readable carrier. Other embodiments comprise the computer program for performing one of the methods described herein, stored on a machine-readable carrier. In other words, an embodiment of the present invention is, therefore, a computer program having a program code for performing one of the methods described herein, when the computer program runs on a computer.

[0140] A further embodiment of the invention provides a storage medium (or a data carrier, or a computer-readable medium) comprising, stored thereon, the computer program for performing one of the methods described herein when it is performed by a processor. The data carrier, the digital storage medium or the recorded medium are typically tangible and/or non-transitionary. A further embodiment of the present invention is an apparatus as described herein comprising a processor and the storage medium.

[0141] A further embodiment of the invention provides a data stream or a sequence of signals representing the computer program for performing one of the methods described herein. The data stream or the sequence of signals may, for example, be configured to be transferred via a data communication connection, for example, via the internet.

[0142] A further embodiment of the invention provides a processing means, for example, a computer or a programmable logic device, configured to, or adapted to, perform one of the methods described herein.

[0143] A further embodiment of the invention provides a computer having installed thereon the computer program for performing one of the methods described herein.

[0144] A further embodiment of the invention provides an apparatus or a system configured to transfer (e.g., electronically or optically) a computer program for performing one of the methods described herein to a receiver. The receiver may, for example, be a computer, a mobile device, a memory device, or the like. The apparatus or system may, for example, comprise a file server for transferring the computer program to the receiver.

[0145] In some embodiments, a programmable logic device (for example, a field programmable gate array) may be used to perform some or all of the functionalities of the methods described herein. In some embodiments, a field programmable gate array may cooperate with a microprocessor in order to perform one of the methods described herein. Generally, the methods are preferably performed by any hardware apparatus.

REFERENCE SIGNS

[0146]

101, ..., 108	access decision point
201, ..., 212	access enforcement point
201a, ..., 212a	access point
301, ..., 304	user
301a, ..., 304a	authentication medium
S01	harvesting ambient light and generating a solar cell signal
S02	determining that a solar cell signal satisfies a mode switching condition
S03	switching the access enforcement point into an active mode
S04	sending an instruction request
S05	receiving an instruction request
S06	causing operation of the access point

Claims

1. A computer-implemented wakeup method performed by an access enforcement point (201),

   wherein the access enforcement point (201) is configured to cause operation, preferably unlocking and/or locking, of an access point (201a),
   wherein the access enforcement point (201) comprises energy harvesting means including a solar cell and an energy storage, the method comprising:

      harvesting (S01) ambient light and generating, by the solar cell, a solar cell signal,
      determining (S02) that the solar cell signal

satisfies a mode switching condition,

in response to determining (S02) that the solar cell signal satisfies a mode switching condition: switching (S03) the access enforcement point (201) from a sleep mode into an active mode,

wherein the mode switching condition comprises a drop of the solar cell signal corresponding to a reduction of ambient light incident on the solar cell that may occur upon, preferably manually, masking the solar cell.

2. The computer-implemented wakeup method according to claim 1, wherein the method further comprises: upon switching (S03) the access enforcement point (201) into an active mode: sending (S04), by the access enforcement point, an instruction request.

3. The computer-implemented wakeup method according to claim 1 or claim 2, wherein the method further comprises:

receiving (S05), by the access enforcement point (201) being in the active mode, an instruction, preferably in response to sending (S04) the instruction request;

wherein the instruction includes an operation-command to cause operation of the access point (201a), and wherein the method further comprises:

causing (S06), by the access enforcement point (201), operation of the access point (201a) according to the instruction.

4. The computer-implemented wakeup method according to claim 3,

wherein the instruction is received from an authentication medium (301a), preferably a mobile device or a physical keycard,

wherein the instruction includes a credential,

wherein prior to causing (S06) operation of the access point (201a), a validity of the credential is determined and operation of the access point (201a) is only caused upon determining that the credential is valid;

or

wherein the instruction includes a command to cause operation of the access point (201a) independent of determining a validity of the credential.

5. The computer-implemented wakeup method according to claim 3, wherein the instruction is received (S05) from an access decision point (101) and wherein the access decision point (101) is configured to:

receive the instruction request sent by the access enforcement point (201),

receive a signal of an authentication medium (301a) of a user (301),

determine an intent of the user (301) to operate the access point (201a), upon receiving the signal of the authentication medium (301a),

generate the instruction dedicated to the access enforcement point (201), upon determining the intent of the user, and

send the instruction to the access enforcement point (201).

6. The computer-implemented wakeup method according to claim 5,
wherein the access decision point (101) is configured to:

receive a credential, preferably from an authentication medium, and

determining a validity of the credential;

wherein preferably, determining the validity of the credential is included in the determining of the intent of the user (301) to operate the access point (201a),

wherein preferably, the access decision point (101) is configured to only generate and/or send the instruction if the credential is determined to be valid.

7. The computer-implemented wakeup method according to any of claims 3 to 6,

wherein the method further comprises: upon receiving (S05) the instruction and/or after causing (S06) operation of the access point (201a), switching the access enforcement point (201) from the active mode to the sleep mode,

wherein preferably, the method further comprises a dead time after switching the access enforcement point (201) from the active mode to the sleep mode,

wherein during the dead time, switching from the sleep mode to the active mode is prevented.

8. The computer-implemented wakeup method according to claim any of claims 1 to 7,
wherein the mode switching condition is based on the signal of the solar cell dropping below a first solar cell dropping threshold and/or dropping by a second solar cell dropping threshold.

9. The computer-implemented wakeup method according to any of claims 1 to 8,

wherein the mode switching condition is adjusted depending on the solar cell signal,

wherein claim 9 preferably depends on claim 8 and the first solar cell dropping threshold and/or the second solar cell dropping threshold are adjusted based on the solar cell signal at a time before the solar cell signal satisfies the mode switching condition.

10. The computer-implemented wakeup method according to any of claims 1 to 9,

wherein the mode switching condition depends on an energy storage level of energy stored in the energy storage,
wherein preferably, the mode switching condition is adjusted depending on the energy storage level,
wherein more preferably, the mode switching condition is relaxed at a higher energy storage level and/or tightened at a lower energy storage level.

11. The computer-implemented wakeup method according to any of claims 1 to 10,
wherein the method further comprises:

charging the energy storage, using the solar cell, wherein the solar cell is deliberately irradiated by a user (301) using a light source,
wherein the mode switching condition is based on the charging, preferably based on the solar cell signal exceeding a charging solar cell threshold and/or based on the energy storage exceeding an energy storage threshold.

12. Use of an access enforcement point (201) in a computer-implemented wakeup method according to any of claims 1 to 11, the access enforcement point (201) including:

energy harvesting means comprising an energy storage and a solar cell;
a communication interface, preferably for communicating with an access decision point (101) and/or an authentication medium (301a);
preferably means for causing operation of an access point (201a); and
processing means for determining that a signal of the solar cell corresponds to a mode switching condition and for switching the access enforcement point (201) from a sleep mode into an active mode.

13. An access enforcement point,

wherein the access enforcement point (201) comprises energy harvesting means;
wherein the energy harvesting means comprise an energy storage and a solar cell;
wherein the access enforcement point (201) is adapted to perform the following actions:

- determine (S02) that a signal of the solar cell satisfies a mode switching condition,
- switch (S03) the access enforcement point (201) from a sleep mode into an active mode, and
- preferably cause (S06) operation of an access point,

wherein preferably, the access enforcement point (201) is configured to be used in a computer-implemented wakeup method according to any of claims 1 to 11.

14. An access control system, comprising:

at least one access enforcement point (201),
at least one an access point (201a),
wherein one of the at least one access enforcement point (201) comprises energy harvesting means including a solar cell and an energy storage,
wherein the system is configured to perform a computer-implemented wakeup method according to any of claims 1 to 11.

15. A computer program comprising computer-readable instructions which when executed by a data processing system cause the data processing system to perform the computer-implemented wakeup method according to any of claims 1 to 11.

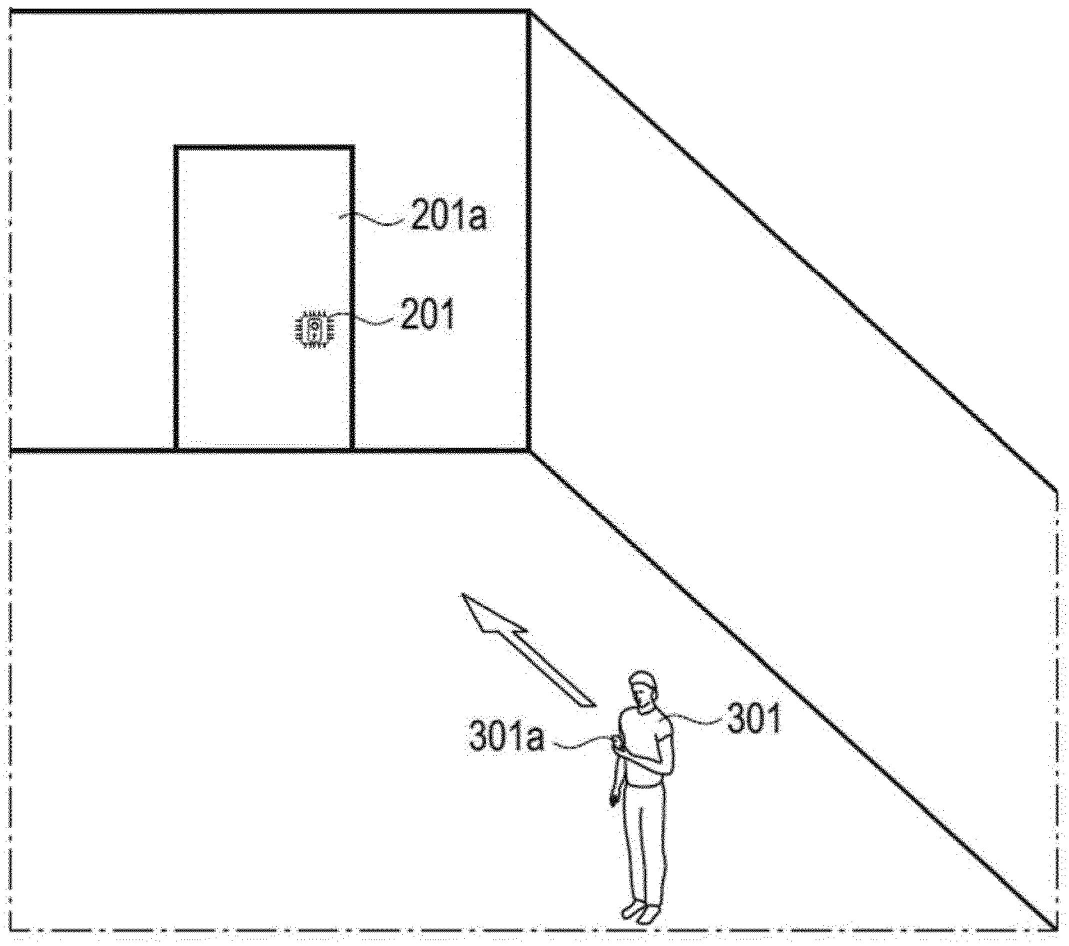
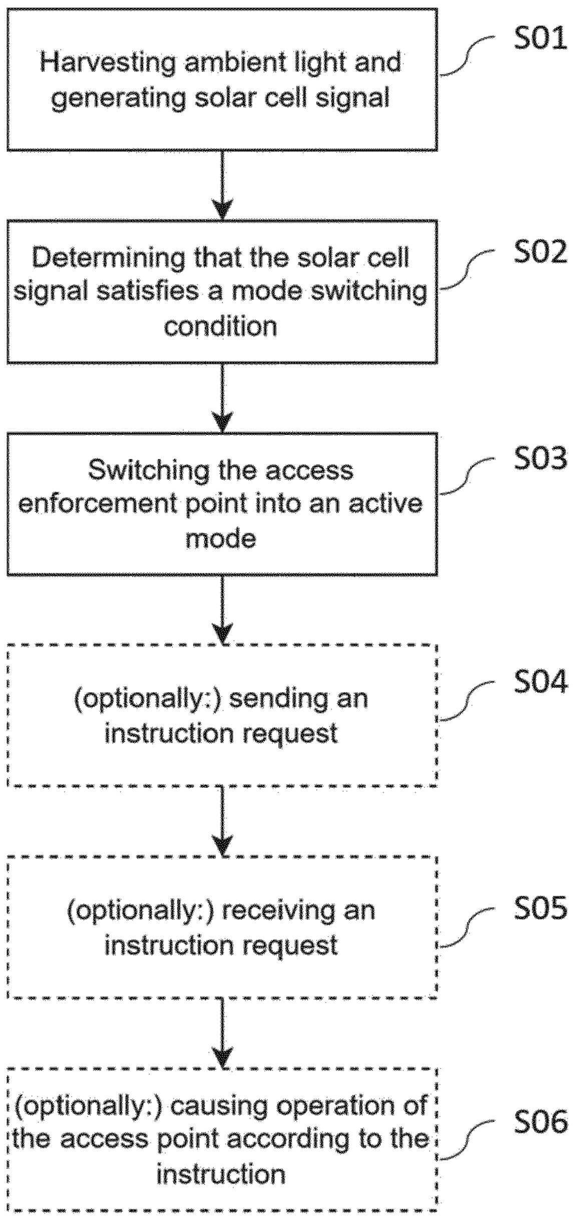


Fig. 1



Harvesting ambient light and generating solar cell signal
S01
Determining that the solar cell signal satisfies a mode switching condition
S02
Switching the access enforcement point into an active mode
S03
(optionally:) sending an instruction request
S04
(optionally:) receiving an instruction request
S05
(optionally:) causing operation of the access point according to the instruction
S06

Fig. 2

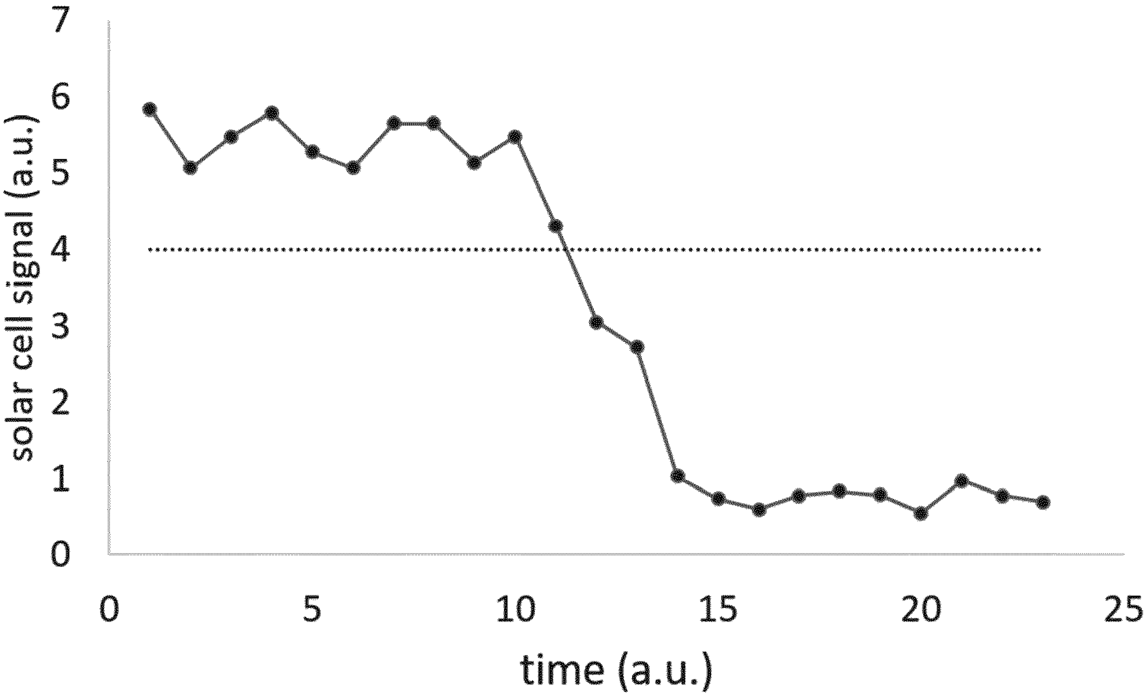


Fig. 3A

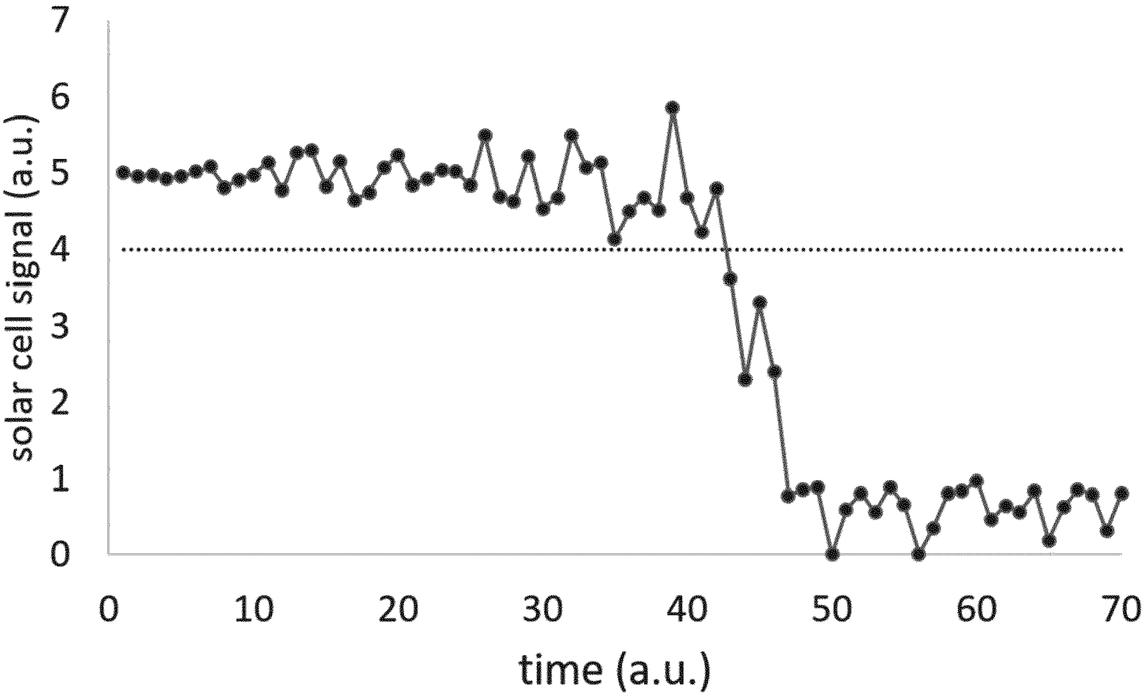


Fig. 3B

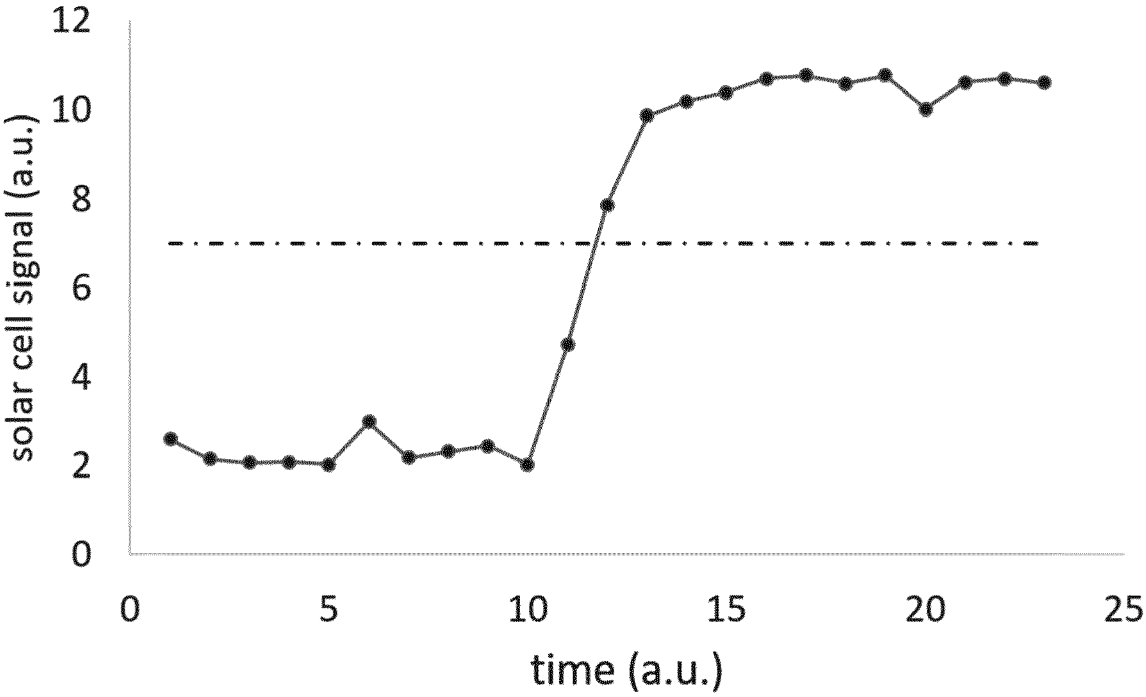


Fig. 3C

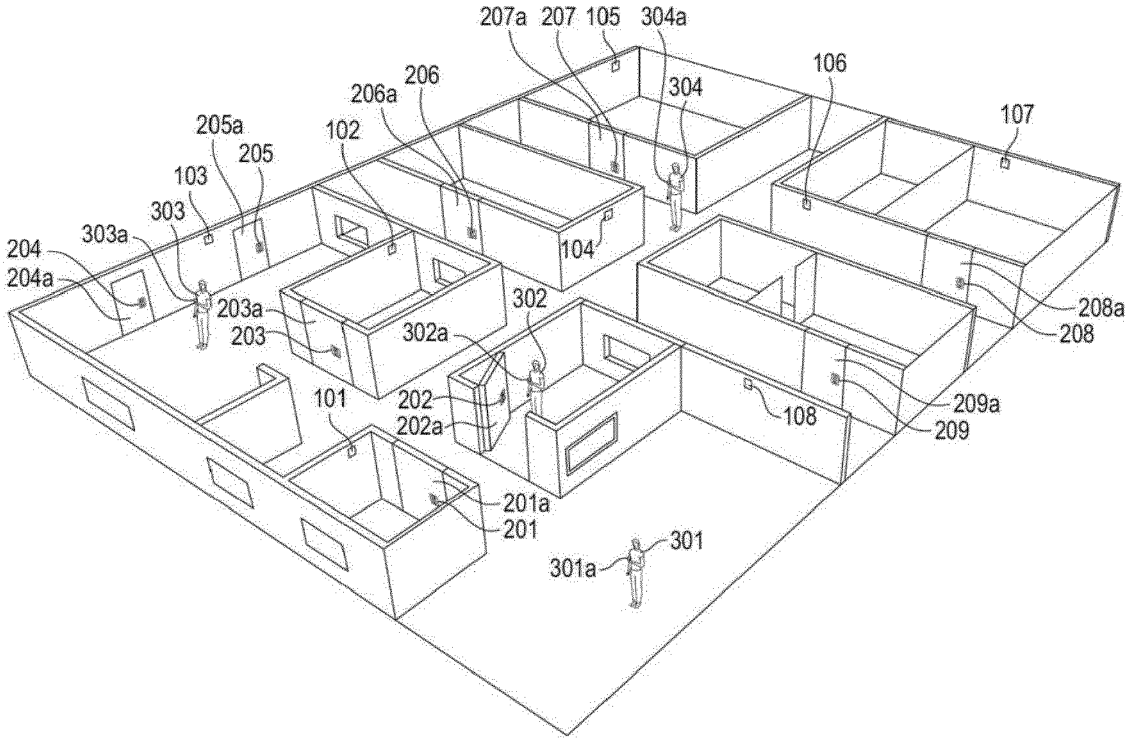

207a
207
105
304a
106
304
107
206
206a
205a
102
205
103
303
303a
104
204
204a
203a
203
302
302a
202
202a
101
108
201a
201
301
301a
208a
208
209a
209

Fig. 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 16 6638

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y	WO 2011/112139 A1 (QURE AB [SE]; SJOEDIN TOR [SE]; MICHAEL PALM [SE]) 15 September 2011 (2011-09-15) * abstract * * page 1, line 12 - page 2, line 13 * * page 5, line 14 - page 9, line 13 * * page 10, line 32 - page 13, line 12 * * claim 1; figures * -----	1,3,4,8, 11-15 2,5-7,9, 10	INV. G07C9/00
Y A	US 2019/387473 A1 (LANG MICHAEL [US] ET AL) 19 December 2019 (2019-12-19) * abstract * * paragraph [0001] - paragraph [0017] * * paragraph [0039] - paragraph [0055] * * figures * -----	2,5-7 1	
Y	US 2015/372536 A1 (NASKALI MATTI JUHANI [JP] ET AL) 24 December 2015 (2015-12-24) * abstract * * paragraph [0001] - paragraph [0006] * * paragraph [0009] - paragraph [0023] * -----	9,10	
			TECHNICAL FIELDS SEARCHED (IPC)
			G07C

The present search report has been drawn up for all claims

1

Place of search	Date of completion of the search	Examiner
The Hague	15 September 2023	Miltgen, Eric

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 23 16 6638

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

15-09-2023

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2011112139 A1	15-09-2011	SE 1050215 A1	09-09-2011
		WO 2011112139 A1	15-09-2011
US 2019387473 A1	19-12-2019	CA 3054793 A1	07-09-2018
		CN 110383900 A	25-10-2019
		EP 3590284 A1	08-01-2020
		US 2019387473 A1	19-12-2019
		US 2020383056 A1	03-12-2020
		WO 2018160343 A1	07-09-2018
US 2015372536 A1	24-12-2015	CN 106463986 A	22-02-2017
		EP 3158620 A1	26-04-2017
		JP 6243556 B2	06-12-2017
		JP 2017520051 A	20-07-2017
		US 2015372536 A1	24-12-2015
		WO 2015193540 A1	23-12-2015

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82