

AN ACCESS CONTROL METHOD

TECHNICAL FIELD

This invention relates generally to an access control method.

5

Background

Currently when the elderly lives alone, away from their loved ones, there can be instances where unfortunate events occur to the elderly, for example, when the elderly experiences a stroke or faints. In such situations, a care giver dispatched to the premise will most often arrive to find a locked door. Hiding the key tucked outside the premise of the elderly may expose the premises to security issue like access to the key, and hence the premise, by an intruder. Even when a spare key is available at a central location, precious time is required for the caregiver to travel to the central location to retrieve the key. In the event when the caregiver is not able to respond to the event, an alternative responder may not be familiar with the location for retrieval of the key. The inconvenience in the need to return the key after use or the key not being returned after use contributes to the inefficacy of having the key placed at a central location. This scenario is replayed in other settings, for example a commercial building, a premise or property overseen by security services or other types of properties and institutions, with the elderly being possibly any individuals to whom help may be rendered. Therefore, there exists a need for a method for addressing the foregoing problems.

10
15
20

Summary

Aspects of the invention is applicable to premises in any setting, including but not limited to landed premises, premises within temporary or mobile structures, premises in commercial buildings or public institutions and the like premises where control of third party access to the premise, for example for aiding, reaching or securing the premise or the occupant of the premise, may be controlled.

25

In accordance with an aspect of the invention, there is disclosed an access control method comprising generating a challenge code in response to an alert event being triggered for a premise and detecting proximity of a communication device to a handling apparatus associated with the premise. The access control method further comprises enabling capture
5 of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being detected and authenticating the captured responder code with the challenge code. A key is retrievable from the handling apparatus in response to the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for gaining access to
10 the premise therevia.

In accordance with a second aspect of the invention, there is disclosed an access control system comprising a control computer system for generating a challenge code in response to an alert event being triggered for a premise, and a handling apparatus for detecting
15 proximity of a communication device to a handling apparatus associated with the premise and for enabling capture of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being detected. The handling apparatus is in data communication with the control computer system with the captured responder code with the challenge code by one of the control computer system and
20 the handling apparatus. Wherein a key is retrievable from the handling apparatus in response to the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for gaining access to the premise therevia.

In accordance with a third aspect of the invention, there is disclosed an alert event verification control method comprising detecting activation of an alert event associated with a premise. The premise comprises at least one image capture device for capturing audio-visual (AV) data from the premise for transmission to at least one communication device for verifying the alert event therevia. The method further comprises initiating a response time window in response to the alert event being activated and capturing AV data from the premise by the at least one image capture device for transmission to the at least one communication device in absence of a cancel request being received from at least one of the premise and the at least one communication device during the response time window.

In accordance with a fourth aspect of the invention, there is disclosed an access control method comprising detecting activation of an alert event associated with a premise, the premise comprising at least one image capture device for capturing audio-visual (AV) data from the premise for transmission to at least one communication device for verifying the alert therevia, determining AV access permission in relation to the premise and generating a challenge code in response to the alert event being triggered for the premise, detecting proximity of a communication device to a handling apparatus associated with the premise, enabling capture of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being detected, and authenticating the captured responder code with the challenge code. Wherein AV data is captured from the premise by the at least one image capture device for transmission to the at least one communication device in response to the AV access permission being received from at least one of the premise and the at least one communication device, and a key is retrievable from the handling apparatus in response to the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for gaining access to the premise therevia.

Brief Description of the Drawings

FIG. 1 shows a system diagram of an access control system according to an aspect of the invention;

5 FIG. 2 shows a data flow diagram of the access control system of FIG. 1;

FIG. 3 illustrates a responder list utilized in the access control system of FIG. 1;

FIG. 4 shows a process flow diagram of an access control method according to an aspect of
10 the invention and implementable by the verification system of FIG. 1; and

FIG. 5 shows a process flow diagram of a warning routine implementable with the access control method of FIG. 4.

Detailed Description

An exemplary embodiment of the present invention, an access control method 100, preferably implemented using an access control system 20, is described hereinafter with reference to FIG. 1 to FIG. 5. The access control system 20 comprises a control computer system 22 or a plurality of inter-networked control computer systems residing on a cloud platform. The control computer system 22 is in data communication with one or more event monitoring systems 24 associated with a plurality of premises 26 to be monitored by each thereof, or to a central control system 28 which manages communication with and control signals to the event monitoring systems 24. Communication between the control computer system 22, the event monitoring systems 24 and the central control system 28 can occur through wired or wireless means. The controller 22 is preferably also in signal and data communication with control computer systems 28 over a network 30. The central control system 28 may also reside on a cloud platform.

In an implementation of the access control system 20, the access control method 100 initiates with generating a challenge code 30 in response to an alert event 32 being triggered by a premise in issue in a step 102. The premise in issue is one of the premises 26. The alert event 32 is triggered by the event monitoring system 24 associated with the one of the premises 26. The event monitoring system 24 monitors the premise 26 through the use of an array of sensors 34, for example temperature sensors, motion sensors, proximity sensors, infrared cameras, video camera and PID switches, ultrasound-based sensors, lux-meters and microphones, for monitoring the premise 26. The alert event 32 triggered through an automated process by the event monitoring system 24 is usually in response to occurrences of situations of concern with the premise in issue, for example the detection of fall or prolonged inactivity of an occupant of the premise in issue 26. Alternatively or in addition to the alert event 32 being triggered by the event monitoring system 24, the alert event 32 may be sent to the central control system 28 for verification by an automated process or by an operator of the central control system 28 to verify the occurrence of the situations of concern.

Based on the type of situations, the event monitoring system 24 may determine if the alert event 32 is to be sent to just the access control system 20 alone, the central control system 28 alone, or to both systems with the central control system 28 sending an independent alert event 32 to the access control system 20 upon verification of the event. For example, a situation triggered by activation of a help button or distress button may be sent directly to the access control system 20, while a fall detected by sensors or camera systems within the premise in issue may be sent to the central control system 28. Nonetheless, all situations and alert events 32 originating from any the event monitoring system 24 are preferably logged with and monitored by the control computer system 22 and the central computer system 28 for response. In some implementations, the control computer system 22 and the central computer system 28 may be physically and functionally merged or integrated. The origin of the alert event 32 received by the access control system 20 is identifiable therefrom and may be tagged with an identifier to identify origin of the alert event 32.

Once the challenge code 30 has been generated, the control computer system 22 identifies one or more responder 36 from a responder list 38 associated with the premise in issue in a step 104. The responder list 38 contains a list of individuals 40 with contact information 42 associated with each of the individuals. The contact information 42, for example phone numbers, device machine address (for example, device IMEI), user sign in address, certificate assigned to the communication device 44, email addresses and identity details of the individuals 40, are for use by the control computer system 22 for establishing communication with communication devices 44 associated with the corresponding one or more individuals 40 on the responder list 38. Each of the individuals 40 listed on the responder list 38 has a priority rank 46 assigned thereto. It is preferred that the different individuals 40 listed on the responder list 38 will have different priority ranks. However, it is not precluded that more than one individual 40 on the responder list 38 may have the same priority rank 46. The individuals 40 can include a call center or a duty personnel at a call center, emergency response center or ambulance service with the communication device 44 associated therewith being a duty-assigned smart device, smart phone or mobile phone.

Further, the control computer system 22 also generates a responder code 48 from the challenge code 30. The responder code 48 can be the challenge code 30 or can be generated from the challenge code 30 using a predetermined function and is matchable or authenticable against the challenge code 30. The responder code 48 can either be a textual
5 codes or machine codes receivable by the communication device 44.

In a step 106, the responder code 48 is sent to the communication device 44 of the individual 40 with the highest priority rank 46 on the responder list 38. In one implementation of the access control method 100, the one or more individual 40 with the
10 highest priority rank is automatically appointed the responder 36 with the responder code 48 being automatically sent to the communication devices 44. In some implementations, the one or more individuals 40 may respond with a “reject” or “unavailable” response through the use of an app operating on the communication devices 44 thereof or through reply message containing a code indicative of rejection or unavailability. If a “reject” or
15 “unavailable” response is received from one or more of the communication devices 44, the access control system 20 selects the individuals with the next highest priority rank 46. This goes on until a responder 36 can be identified. In other implementations, an “acknowledgement” or “accept” response is required to be received from the communication device 44 of the selected individuals 40 on the responder list 38 within a
20 predefined response duration 52, failing which, the control computer system 22 will select the individuals with the next highest priority rank 46. This also goes on until a responder 36 can be identified. If no responder 36 can be identified, the control computer system 22 can have a default protocol of, for example, informing the ambulance service or inform event monitoring system 24 that no responder 36 can be identified.

25

Next, proximity between the communication device 44 of the responder 36 and a handling apparatus 52 is determined in a step 108. The handling apparatus 52 is preferably located within the vicinity of the premise in issue 26. For example, the handling apparatus 52 can be located either next to an entrance of the premise in issue 26 or at a common access point
30 or lobby leading to the premise in issue 26.

Proximity between the communication device 44 of the responder 36 and the handling apparatus 52 can be determined by determining geo-location of the communication device 44 to thereby determine distance thereof from the handling apparatus 52. Geo-location data for the communication device 44 and the handling apparatus is obtainable through GPS,
5 A/GPS, WiFi and the like geo-location data sources.

Alternatively, proximity between the communication device 44 of the responder 36 and the handling apparatus 52 can be determined by detecting signaling for association sent from the communication device 44 by the handling apparatus 52. Once proximity between the
10 communication device 44 of the responder 36 and the handling apparatus 52 has been detected, identity data 56 is procured by the handling apparatus 52 from the communication device 44 in a step 110. The identity data 56 enables the identity of the responder 36 to be verified and can be performed by send the identity data 56 back to the control computer system 22 for verification against the contact information 42 of the responder 36, or can be
15 authenticated by the handling apparatus 52 against the contact information 42 of the responder 36 downloaded from the control computer system 22. Once the identity data 56 has been authenticated, a data communication pathway is established between the communication device 44 and the handling apparatus 52 in a step 112.

20 Next, capture of the responder code 48 by the handling apparatus 52 is enabled in a step 120 in response to proximity of the communication device 44 to the handling apparatus 52 being detected. The step 120 comprises enabling capture of the responder code 48 received as data wirelessly communicated from the handling apparatus 52 to the communication device 44. Wireless communication between the handling apparatus 52 and the communication
25 device 44 can occur through various known wireless communication means and protocols including but not limited to Bluetooth, near-field communication (NFC) and WiFi communication. The responder code 48 communicated from the communication device 44 to the handler apparatus 52 can be communicated as textual data, machine code or encrypted certificate data.

The step 120 can further or alternatively comprise enabling capture of the responder code 48 from a user interface (UI) 58 of the handling apparatus 52 when the responder 36 interacts therewith. Preferably, the UI 58 comprises at least one of a key pad, a touch screen, an image capture device and a thermal sensor array for capturing key-presses, touch input or gestures from the responder 36. Further alternatively in the step 120, the handling apparatus 52 may initiate an application on the communication device 44 to enable capture of the responder code 48 from the responder 36 who has already received the responder code 48 as a textual code through a message service, a secondary device or via other means.

Once the responder code 48 has been received by the handling apparatus 52, the captured responder code 48 is authenticated against the challenge code 30 by the handling apparatus 52 or the control computer system 22 in a step 122. Upon positive authentication of the captured responder code 48, a key 60 is presented for retrieval by the responder 36 in a step 130. In situations where non-responder intervention is required, the control computer system 22 can be requested to present the key 60 for retrieval even when positive authentication of the responder code 48 does not or is not able to occur.

The key 60 is for gaining access through the entrance of the premise in issue 26. The entrance comprises a lock system 62 which has to be deactivated or unlocked using the key 60 in order to enable opening of a door at the entrance. Preferably, the key 60 is one of a physical key for unlocking a door at the entrance of the premise 26. Alternatively, the key 60 is a transponder device, for example an RFID tag or card, for wireless unlocking of the lock system 62 at a premise 26. Further alternatively, the key 60 is a data storage device, for example a USB storage device, containing an access code and couplable to the lock system 62 for unlocking the lock system 62.

Preferably, the handling apparatus 52 comprises a controller 64 and a communication module 66 for establishing communications, by wired and wireless means, with the control computer system 22 and the communication device 44.

The handling apparatus 52 further comprises a handling mechanism 68 to enable dispensing, presenting, collecting and reception of the key 60 to be effected. The handling mechanism 68 can comprise a dispensing chute where the key 60 can be dispensed into for retrieval by the responder 36 and a collection chute whereto the key 60 can be placed or dropped into after use thereof. Alternatively or in addition, the handling mechanism 68 can comprise a pick-and-place actuator assembly with an end-effector, for example a mechanical gripper, a vacuum-based picker or an electro-magnetic picker, for handling the key 60 during dispensing and collection thereof. The key 60 can be tagged with an RFID tag or a machine readable code, for example a bar code or a QR code, directly thereonto or indirectly onto a key chain whereto the key is attachable. Tagging of the key 60 enables the key to be identified during dispensing and collection especially when one single handling apparatus 52 is used for handling keys to multiple premises. Tagging of key is also important even when a dedicated handling apparatus 52 is used for a single premise as it ensures that the correct key 60 is collected by thereby for subsequent use. Further alternatively, the handling mechanism 68 can comprise a key cabinet with multiple receptacle, each for securing, releasing for retrieval and verifying during collection or reception of a tagged key chain whereto the key 60 is coupled.

When the handling mechanism 68 is disposed adjacent or with the door, the handling mechanism 68 can be disposed in front of the door or at the entrance next to the door. However, it is also preferred that the handling mechanism 68 be placed within the premise in issue 26 behind the door. Hence, the handling mechanism 68 may be coupled to the door or is structurally decoupled from the door to enable the key 60 to be presented by dropping the key onto a surface, for example the floor of the premise, so that the key 60 may be accessed through a gap between the door and the floor. Retrieving of the key 60 through the gap can be effected by sweeping or hooking the key 60 through the gap using available articles like elongated structures or anything that is available and usable for disposing through the gap for retrieving the key 60. By placing the handling mechanism 68 behind the door, the handling mechanism 68 is not only hidden from plain view but also kept away from direct physical access thereto that may encourage or subject the handling mechanism

and the key 60 contained therein from vandalism, damage, manipulation and forced access. This also conveys a better sense of security as opposed to leaving the handling mechanism 68 and consequently the key 60 exposed outside the premise 26 away from the security of being behind the door.

5

In an implementation of the access control method 100 and the access control system 20, the responder list 38 will be populated with a list of individuals 40 with corresponding priority ranks. It is not precluded that the responder list 38 may only contain one individual 40. Assuming that the occupant of the premise 26 is an elderly person, the responder list 38 will contain the name and contact information 42 of a caregiver, the occupant's son, the occupant's daughter and the occupant's friend with exemplary corresponding priority rank 46 of AA, BB, BB and CC respectively. It is noted here that AA is of a higher priority rank than BB, which in turn is of a higher priority rank than CC.

10

15 In the event that the event monitoring system 24 captures an event, for example a fall, an alert event 32 will be triggered and will also be provided to the access control system 20. Prior to sending the alert event 32 to the access control system 20, the event monitoring system 24, or the central control system 28, may require verification of a fall by a duty officer. The duty officer can be on the move/ on patrol and hence will utilized a remote mobile device in data communication with the central control system 28 for viewing, responding to and verifying the alert event 32. The duty officer may remotely activate and access one or more image capture devices 70 installed within the premise 26 to verify that a fall has indeed occurred. In addition, the responder 36 may also be able to remotely activate and access the one or more image capture devices 70 installed within the premise 26 to verify that a fall has indeed occurred or to assess or reconfirm the situation. The image capture devices 70 may constitute a portion of the array of sensors 34. To maintain the privacy of the occupant of the premise, the one or more image capture device 70 can be accessed by the duty officer only when the alert event 32 has been triggered and images, still image or video images, will be processed by applying image blurring techniques, for example Gaussian blurring, prior to being transmitted to the duty officer. Alternative or

20

25

30

additional techniques of occluding the person in the video stream with an avatar may also be applied to protect the vanity of the person/occupant of the premise in issue 26.

As the occupant of the premise and their family or friends may not want audio-visual (AV) data, for example still images, videos and audio data, to be transmitted or provided image capture devices 70 at certain times of the day or from certain areas within the premise 26, an option can be available to enable either the occupant or any of the individuals 40 on the responder list 38 to stop or restrict the transmission. Hence, in some implementations, a warning routine 300 may be implemented where warnings may be activated prior to transmitting any AV data from any of the image capture devices 70 in a step 302. The warnings can be in the form of one or more of activating sirens and alarms located within the premise 26, sending of messages displayed on screens, display devices or computer monitors within the premise, sending an alert message to duty officer and one or more of the communication devices 44 associated with one or more of the individuals 40 on the responder list 38, sending an alert message to at least one wearable device worn by the occupant of the premise 26 or the like warnings to anyone or any system that may have an interest in controlling access to transmissions from the image capture devices 70. Once the warning has been activated, a respond time window or duration is initiated in a step 304 wherein, a cancel request has to be received by the event monitoring system 24 in order for the transmission of the AV data to be cancelled.

If no cancel request has been received at the elapse of the respond time window or duration, transmission of the AV data from the image capture devices 70 will be initiated in a step 306. The AV data will be sent to a duty officer, for example the duty officer at the central control system 28, who assesses if the event requires attention. If the duty officer decides that the event requires no attention or if the event is determined to be a false alarm, the duty officer may, in a step 308, decide not to send the alert event 32 to the access control system 20. If the duty officer determines that attention is required for the event, the alert event 32 will be sent to the access control system 20 in a step 310.

The cancel request can be from a respond message or command from any of the communication devices 44 where to the warning has been sent or cancellation request initiated by the occupant of the premise 26 through gestures, activation of a cancellation pushbutton or audio command. Once a cancel request has been received, transmission of AV data from the image capture devices 70 either ceases or is restricted to only pre-selected regions within the premise in a step 312. In instances where no cancel request has been received within the respond time window, the event monitoring system 24 will send the alert event 32 to the access control system 20 only after the duty officer has verified that something has occurred to the occupant of the premise 26. In instances where one or more cancel request has been received, the event monitoring system 24 will then proceed to immediately send the alert event 32 to the access control system 20 in the step 310.

The above approach can be implemented through use of a machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to detect activation of an alert event associated with a premise with the premise comprising at least one image capture device for capturing audio-visual (AV) data from the premise for transmission to at least one communication device for verifying the alert therevia. The plurality of programming instructions, when executed, further cause the machine to initiate a response time window in response to the alert event being activated and capture AV data from the premise by the at least one image capture device for transmission to the at least one communication device in absence of a cancel request being received from at least one of the premise and the at least one communication device during the response time window.

The above approach can be alternatively implemented through use of a machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to detect activation of an alert event associated with a premise, the premise comprising at least one image capture device for capturing audio-visual (AV) data from the premise for transmission to at least one communication device for verifying the alert therevia, determine AV access permission in relation to the

premise and generating a challenge code in response to the alert event being triggered for the premise, detecting proximity of a communication device to a handling apparatus associated with the premise, enable capture of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being
5 detected, and authenticate the captured responder code with the challenge code. Wherein the AV data is captured from the premise by the at least one image capture device for transmission to the at least one communication device in response to the AV access permission being received from at least one of the premise and the at least one communication device, and a key is retrievable from the handling apparatus in response to
10 the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for gaining access to the premise therevia. Further, determining AV access permission in relation to the premise can comprise initiating a response time window in response to the alert event being activated, wherein AV data is captured from the premise by the at least one image capture device for transmission to the at
15 least one communication device in absence of a cancel request being received from at least one of the premise and the at least one communication device during the response time window. In the event where AV access permission is not received or AV access permission is explicitly refused, access to the at least one image capture device for capturing the AV data is impeded or disallowed.

20

Once the alert event 32 has been received by the access control system 20, the access control system will generate the challenge code 30 and the corresponding responder code 48 from the challenge code 30. The responder code 48 is then sent to the communication device 44
25 of the individual 40 with the highest priority rank 46, who happens to be the caregiver, in this example. Assuming that no response is received from the caregiver, the responder code 48 with then be sent to both the communication devices 44 of both the occupant's son and the occupant's daughter since both of them have the same priority rank 46 of BB. Assuming that the occupant's son respond but the occupant's daughter does not, the occupant's son
30 will be deemed or assigned as the responder 36.

The handling apparatus 52 will then be primed to detect proximity of the communication device 44 of the occupant's son thereto. In the event the communication device 44 may not be able to communicate with the handling apparatus 52 due to hardware or software problems, the responder 36 may call the duty officer to remotely allow bypass of the proximity sensing step 108 and enable the access control system to capture the responder code 48 from the responder via the UI 58. The duty officer may require a pre-determined verbal password or code to be provided by the responder 36 in order for the bypassing of the proximity sensing step 108 to be bypassed.

Once proximity of the communication device 44 of the responder 36 has been detected, the handling apparatus will enable capture of the responder code 48 wirelessly or via session certificate exchange with the communication device 44 of the responder 36 or through capture of the responder code 48 via the UI 58. Once the responder code 48 has been captured by the handling apparatus 52 and positively authenticated, the key 60 will then be presented by the handling mechanism 68 for retrieval by the responder 36, the occupant's son, to enable him to unlock the lock system 62 so that the door at the entrance to the premise in issue 26 can be opened to allow the occupant's son to access the premise in issue 26 and tend to the occupant. The handling apparatus 52 can further comprise a camera array 72 strategically placed for capturing images of the person, in this case the responder 36, who accesses the key 60.

The access control method 100 may be implemented through use of a machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to generate a challenge code in response to an alert event being triggered for a premise and detect proximity of a communication device to a handling apparatus associated with the premise. The plurality of programming instructions, when executed, further cause the machine to enable capture of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being detected and authenticate the captured responder code with the

challenge code. Wherein a key is retrievable from the handling apparatus in response to the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for gaining access to the premise therevia.

- 5 Aspects of particular embodiments of the present disclosure address at least one aspect, problem, limitation, and/or disadvantage associated with existing access control methods and systems. While features, aspects, and/or advantages associated with certain embodiments have been described in the disclosure, other embodiments may also exhibit such features, aspects, and/or advantages, and not all embodiments need necessarily exhibit
- 10 such features, aspects, and/or advantages to fall within the scope of the disclosure. It will be appreciated by a person of ordinary skill in the art that several of the above-disclosed structures, components, or alternatives thereof, can be desirably combined into alternative structures, components, and/or applications. In addition, various modifications, alterations, and/or improvements may be made to various embodiments that are disclosed by a person of
- 15 ordinary skill in the art within the scope of the present disclosure, which is limited only by the following claims.

Claims

1. An access control method comprising:
 - generating a challenge code in response to an alert event being triggered for a premise;
 - 5 detecting proximity of a communication device to a handling apparatus associated with the premise;
 - enabling capture of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being detected; and
 - 10 authenticating the captured responder code with the challenge code, wherein a key is retrievable from the handling apparatus in response to the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for gaining access to the premise therevia.
 - 15
2. The access control method as in claim 1, further comprising:
 - presenting the key for retrieval by a responder.
3. The access control method as in 1, generating a challenge code in response to an
 - 20 alert event being triggered for a premise comprising:
 - receiving an alert event by a control system, the alert event being triggered from the premise; and
 - generating the challenge code by the control system.
- 25 4. The access control method as in 1, generating a challenge code in response to an alert event being triggered for a premise comprising:
 - sending the responder code to the communication device, the responder code being generated from the challenge code.

5. The access control method as in 1, detecting proximity of a communication device to a handling apparatus associated with the premise comprising:

determining geo-location of the communication device to thereby determine distance thereof from the handling apparatus.

5

6. The access control method as in 1, detecting proximity of a communication device to a handling apparatus associated with the premise comprising:

detecting signaling for association from the communication device by the handling apparatus.

10

7. The access control method as in 6, detecting proximity of a communication device to a handling apparatus associated with the premise further comprising:

procuring identity data from the communication device in response to signaling for association being detected by the handling apparatus; and

15

establishing a data communication pathway between the communication device and the handling apparatus in response to the identity data being verified.

8. The access control method as in 7, enabling capture of a responder code by the handling apparatus in response to proximity of the device to the handling apparatus being detected comprising:

20

enabling capture of a responder code by the handling apparatus further in response to data communication pathway between the communication device and the handling apparatus being established.

25

9. The access control method as in 1, enabling capture of a responder code by the handling apparatus in response to proximity of the device to the handling apparatus being detected comprising:

enabling capture of the responder code from a responder when a responder interacts with a user interface (UI) of the handling apparatus.

30

10. The access control method as in 9, the UI comprising at least one of a key pad, a touch screen, an image capture device and a thermal sensor array.
- 5 11. The access control method as in 1, enabling capture of a responder code by the handling apparatus in response to proximity of the device to the handling apparatus being detected comprising:
enabling capture of the responder code received as data wirelessly communicated from the handling apparatus to the communication device.
- 10 12. The access control method as in 1, the key being one of a physical key for unlocking a door at the entrance of the premise, a transponder device for wireless unlocking of a door at a premise and a data storage device containing an access code for unlocking door.
- 15 13. The access control method as in 12, the transponder device comprising an RFID tag.
14. The access control method as in 2, further comprising:
receiving the key from the responder subsequent to a door at the entrance of the premise being unlocked thereby.

15. An access control system comprising:

a control computer system for generating a challenge code in response to an alert event being triggered for a premise; and

5 a handling apparatus for detecting proximity of a communication device to a handling apparatus associated with the premise and for enabling capture of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being detected, the handling apparatus being in data communication with the control computer system, the
10 captured responder code being authenticated with the challenge code by one of the control computer system,

wherein the handling apparatus and a key is retrievable from the handling apparatus in response to the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for
15 gaining access to the premise therevia.

16. The access control system as in claim 15, the handling apparatus further for presenting the key for retrieval by a responder.

20 17. The access control system as in 15, the control computer system generates the responder code from the challenge code for sending to the communication device.

18. The access control system as in 15, one of the control computer system and the handling apparatus detects proximity of a communication device to the handling
25 apparatus associated with the premise by at least one of determining geo-location of the communication device to thereby determine distance thereof from the handling apparatus and detecting signaling for association from the communication device by the handling apparatus.

19. The access control system as in 15, the handling apparatus comprises a user interface (UI) for enabling capture of the responder code from a responder when the responder interacts therewith.
- 5 20. The access control system as in 19, the UI comprising at least one of a key pad, a touch screen, an image capture device and a thermal sensor array.
21. The access control system as in 15, the handling device comprising a communication module for enabling capture of the responder code received as data wirelessly
10 communicated from the handling apparatus to the communication device.
22. The access control system as in 15, the key being one of a physical key for unlocking a door at the entrance of the premise, a transponder device for wireless unlocking of a door at a premise and a data storage device containing an access code for
15 unlocking door.
23. The access control system as in 22, the transponder device comprising an RFID tag.
24. The access control system as in 16, the handling device further for receiving the key
20 from the responder subsequent to a door at the entrance of the entrance being unlocked thereby.

25. An alert event verification control method comprising:
- 5 detecting activation of an alert event associated with a premise, the premise comprising at least one image capture device for capturing audio-visual (AV) data from the premise for transmission to at least one communication device for verifying the alert therevia;
- initiating a response time window in response to the alert event being activated; and
- 10 capturing AV data from the premise by the at least one image capture device for transmission to the at least one communication device in absence of a cancel request being received from at least one of the premise and the at least one communication device during the response time window.
26. The method as in claim 25, the AV data comprising still images, videos and audio data.
- 15
27. The method as in claim 25, initiating a response time window in response to the alert event being activated comprising:
- 20 sending a warning message to at least one of the premise and the at least one communication device.
28. The method as in claim 27, sending a warning message to the premise comprising at least one of activating audio and visual indicators within the premise, sending the warning messages to display devices within the premise and sending the warning message to at least one wearable device worn by an occupant of the premise.
- 25

29. The method as in claim 25, further comprising:

5 preventing capture of AV data from the premise by the at least one image capture device and transmission of AV data captured by the at least one image capture device to the at least one communication device in response to a cancel request being received from at least one of the premise and the at least one communication device.

30. An access control method comprising:

10 detecting activation of an alert event associated with a premise, the premise comprising at least one image capture device for capturing audio-visual (AV) data from the premise for transmission to at least one communication device for verifying the alert therevia;

15 determining AV access permission in relation to the premise and generating a challenge code in response to the alert event being triggered for the premise;

detecting proximity of a communication device to a handling apparatus associated with the premise;

20 enabling capture of a responder code by the handling apparatus in response to proximity of the communication device to the handling apparatus being detected; and

authenticating the captured responder code with the challenge code,

25 wherein AV data is captured from the premise by the at least one image capture device for transmission to the at least one communication device in response to the AV access permission being received from at least one of the premise and the at least one communication device, and a key is retrievable from the handling apparatus in response to the responder code being authenticated against the challenge code, the key is for use in enabling access through an entrance of a premise for gaining access to the premise therevia.

31. The method as in claim 30, determining AV access permission in relation to the premise comprising:

initiating a response time window in response to the alert event being activated,

- 5 wherein the AV data is captured from the premise by the at least one image capture device for transmission to the at least one communication device in absence of a cancel request being received from at least one of the premise and the at least one communication device during the response time window.